

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.				
1. AGENCY USE ONLY (Leave blank)		2. REPORT DATE 7 June 1996		3. REPORT TYPE AND DATES COVERED Master's Thesis, 31 July 95-7 June 96
4. TITLE AND SUBTITLE Shaping the Battlefield With Command and Control Warfare			5. FUNDING NUMBERS	
6. AUTHOR(S) Major Elizabeth A. Hurst, U.S. Army				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) U.S. Army Command and General Staff College ATTN: ATZL-SWD-GD, 1 Reynolds Avenue Fort Leavenworth, Kansas 66027-6900			8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)			10. SPONSORING / MONITORING AGENCY REPORT NUMBER	
11. SUPPLEMENTARY NOTES DTIC QUALITY INSPECTED 4				
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release, distribution is unlimited.			12b. DISTRIBUTION CODE A	
13. ABSTRACT (Maximum 200 words) This study examines the application of command and control warfare (C2W) as a supporting strategy on the battlefield. It begins with an overview of C2W, discussing its five elements--operations security, military deception, physical destruction, and electronic warfare--and the role they play, both in protecting friendly command and control (C2) and in attacking an opponent's C2. The study underscores the advantages they bring to the battlefield when these elements are synchronized into a mutually supporting strategy whose main focus centers on enhancing the success of the commander's overall objectives. The study examines the Persian Gulf War of 1990 to 1991 to demonstrate an application of C2W. It discusses how the employment of C2W during the Gulf War evolved from the defensive-oriented doctrine of command, control, and communications countermeasures (C3CM) to embrace a more offensive-oriented strategy of attacking the entire enemy information system, including the human element. The study contends that this effective integration and application of C2W's five elements contributed significantly to the unprecedented success of Coalition forces in the Gulf War. It concludes with an analysis of the import this carries for future operations and offers recommendations to optimize unit C2W programs.				
14. SUBJECT TERMS Command and Control Warfare, Information Warfare, Information Operations			15. NUMBER OF PAGES 97	
			16. PRICE CODE	
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT Unlimited	

GENERAL INSTRUCTIONS FOR COMPLETING SF 298

The Report Documentation Page (RDP) is used in announcing and cataloging reports. It is important that this information be consistent with the rest of the report, particularly the cover and title page. Instructions for filling in each block of the form follow. It is important to *stay within the lines* to meet optical scanning requirements.

Block 1. Agency Use Only (Leave blank).

Block 2. Report Date. Full publication date including day, month, and year, if available (e.g. 1 Jan 88). Must cite at least the year.

Block 3. Type of Report and Dates Covered. State whether report is interim, final, etc. If applicable, enter inclusive report dates (e.g. 10 Jun 87 - 30 Jun 88).

Block 4. Title and Subtitle. A title is taken from the part of the report that provides the most meaningful and complete information. When a report is prepared in more than one volume, repeat the primary title, add volume number, and include subtitle for the specific volume. On classified documents enter the title classification in parentheses.

Block 5. Funding Numbers. To include contract and grant numbers; may include program element number(s), project number(s), task number(s), and work unit number(s). Use the following labels:

C - Contract	PR - Project
G - Grant	TA - Task
PE - Program Element	WU - Work Unit Accession No.

Block 6. Author(s). Name(s) of person(s) responsible for writing the report, performing the research, or credited with the content of the report. If editor or compiler, this should follow the name(s).

Block 7. Performing Organization Name(s) and Address(es). Self-explanatory.

Block 8. Performing Organization Report Number. Enter the unique alphanumeric report number(s) assigned by the organization performing the report.

Block 9. Sponsoring/Monitoring Agency Name(s) and Address(es). Self-explanatory.

Block 10. Sponsoring/Monitoring Agency Report Number. (If known)

Block 11. Supplementary Notes. Enter information not included elsewhere such as: Prepared in cooperation with...; Trans. of...; To be published in.... When a report is revised, include a statement whether the new report supersedes or supplements the older report.

Block 12a. Distribution/Availability Statement. Denotes public availability or limitations. Cite any availability to the public. Enter additional limitations or special markings in all capitals (e.g. NOFORN, REL, ITAR).

DOD - See DoDD 5230.24, "Distribution Statements on Technical Documents."

DOE - See authorities.

NASA - See Handbook NHB 2200.2.

NTIS - Leave blank.

Block 12b. Distribution Code.

DOD - Leave blank.

DOE - Enter DOE distribution categories from the Standard Distribution for Unclassified Scientific and Technical Reports.

NASA - Leave blank.

NTIS - Leave blank.

Block 13. Abstract. Include a brief (*Maximum 200 words*) factual summary of the most significant information contained in the report.

Block 14. Subject Terms. Keywords or phrases identifying major subjects in the report.

Block 15. Number of Pages. Enter the total number of pages.

Block 16. Price Code. Enter appropriate price code (*NTIS only*).

Blocks 17 - 19. Security Classifications. Self-explanatory. Enter U.S. Security Classification in accordance with U.S. Security Regulations (i.e., UNCLASSIFIED). If form contains classified information, stamp classification on the top and bottom of the page.

Block 20. Limitation of Abstract. This block must be completed to assign a limitation to the abstract. Enter either UL (unlimited) or SAR (same as report). An entry in this block is necessary if the abstract is to be limited. If blank, the abstract is assumed to be unlimited.

SHAPING THE BATTLEFIELD WITH COMMAND
AND CONTROL WARFARE

A thesis presented to the Faculty of the U.S. Army
Command and General Staff College in partial
fulfillment of the requirements for the
degree

MASTER OF MILITARY ART AND SCIENCE

by

ELIZABETH A. HURST, MAJ, U.S. ARMY
B.A., University of North Carolina, Asheville, North Carolina, 1978

FORT LEAVENWORTH, KANSAS
1996

Approved for public release; distribution is unlimited.

19960820 049

SHAPING THE BATTLEFIELD WITH COMMAND
AND CONTROL WARFARE

A thesis presented to the Faculty of the U.S. Army
Command and General Staff College in partial
fulfillment of the requirements for the
degree

MASTER OF MILITARY ART AND SCIENCE

by

ELIZABETH A. HURST, MAJ, U.S. ARMY
B.A., University of North Carolina, Asheville, North Carolina, 1978

FORT LEAVENWORTH, KANSAS
1996

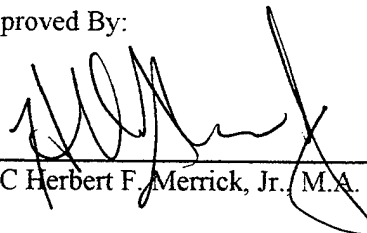
Approved for public release; distribution is unlimited.

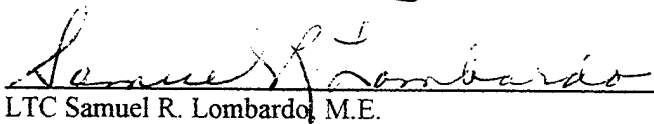
MASTER OF MILITARY ART AND SCIENCE
THESIS APPROVAL PAGE

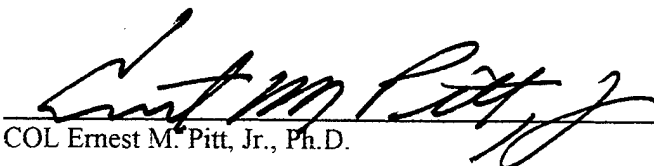
Name of Candidate: MAJ Elizabeth A. Hurst

Title of Thesis: Shaping the Battlefield with Command and Control Warfare

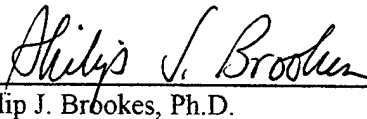
Approved By:


_____, Chairman
LTC Herbert F. Merrick, Jr., M.A.


_____, Member
LTC Samuel R. Lombardo, M.E.


_____, Member, Consulting Faculty
COL Ernest M. Pitt, Jr., Ph.D.

Accepted this 7th day of June 1996 by:


_____, Director, Graduate Degree Programs
Philip J. Brookes, Ph.D.

The opinions and conclusions expressed herein are those of the student author and do not necessarily represent the views of the U.S. Army Command and General Staff College or any other governmental agency. (References to this study should include the foregoing statement.)

ABSTRACT

SHAPING THE BATTLEFIELD WITH COMMAND AND CONTROL WARFARE by MAJ
Elizabeth A. Hurst, USA, 97 pages.

This study examines the application of command and control warfare (C2W) as a supporting strategy on the battlefield. It begins with an overview of C2W, discussing its five elements--operations security, military deception, physical destruction, and electronic warfare--and the role they play, both in protecting friendly command and control (C2) and in attacking an opponent's C2. The study underscores the advantages they bring to the battlefield when these elements are synchronized into a mutually supporting strategy whose main focus centers on enhancing the success of the commander's overall objectives. The study examines the Persian Gulf War of 1990 to 1991 to demonstrate an application of C2W. It discusses how the employment of C2W during the Gulf War evolved from the defensive-oriented doctrine of command, control, and communications countermeasures (C3CM) to embrace a more offensive-oriented strategy of attacking the entire enemy information system, including the human element. The study contends that this effective integration and application of C2W's five elements contributed significantly to the unprecedented success of Coalition forces in the Gulf War. It concludes with an analysis of the import this carries for future operations and offers recommendations to optimize unit C2W programs.

TABLE OF CONTENTS

	Page
THESIS APPROVAL PAGE	ii
ABSTRACT	iii
LIST OF TABLES	v
LIST OF ILLUSTRATIONS	vi
LIST OF ABBREVIATIONS	vii
CHAPTER	
1. INTRODUCTION	1
2. WHAT IS C2W?	18
3. APPLICATION OF C2W: THE GULF WAR	50
4. CONCLUSIONS	79
BIBLIOGRAPHY	90
INITIAL DISTRIBUTION LIST	96

LIST OF TABLES

Table	Page
1. OPSEC Capabilities	28
2. PSYOP Capabilities	31
3. Military Deception Capabilities	35
4. Electronic Warfare Capabilities	38
5. Physical Destruction Capabilities	41
6. Intelligence Support to Command and Control Warfare	43
7. Mutual Support Within C2	81
8. Conflicts Within C2W	82

LIST OF ILLUSTRATIONS

Figure	Page
1. First Strike	1
2. Twelve Hours Later	2

LIST OF ABBREVIATIONS

AAA	Anti-Aircraft Artillery
ARM	Anti-Radiation Missile
ASM	Air-to-Surface Missile
ASUW	Antisurface Warfare
ATACMS	Army Tactical Missile System
ATF	Amphibious Task Force
ATO	Air Tasking Order
AWACS	Airborne Warning and Control System
BDA	Battle Damage Assessment
C2	Command and Control
C2W	Command and Control Warfare
C3	Command, Control, and Communications
C3CM	Command, Control, and Communications Countermeasures
C3I	Command, Control, Communications and Intelligence
CAP	Combat Air Patrol
CENTAF	Air Force Component, Central Command
CENTCOM	Central Command
CEWI	Combat Electronic Warfare and Intelligence
CINCCENT	Commander in Chief, Central Command
CJCS	Chairman, Joint Chiefs of Staff
CNN	Cable News Network
COMINT	Communications Intelligence

COMSEC	Communications Security
DEW	Directed Energy Weapon
DOD	Department of Defense
EA	Electronic Attack
ELINT	Electronics Intelligence
EMCON	Emissions Control
EMP	Electro-Magnetic Pulse
EP	Electronic Protection
EPW	Enemy Prisoner of War
ES	Electronic Support
EW	Electronic Warfare
FLOT	Forward Line of Own Troops
FM	Frequency Modulation / Field Manual
GNP	Gross National Product
HARM	High-Speed Anti-Radiation Missile
HUMINT	Human Intelligence
IADS	Integrated Air Defense System
IBW	Information Based Warfare
IEW	Information Economic Warfare
IO	Information Operations
IW	Information Warfare
MCM	Mine Countermeasures
MEB	Marine Expeditionary Brigade
MOP	Memorandum of Policy
NATO	North Atlantic Treaty Organization
NAVCENT	Naval Component, Central Command

NBC	Nuclear, Biological, and Chemical
NGFS	Naval Gunfire Support
OPSEC	Operations Security
POW	Prisoner of War
PSYOP	Psychological Operations
RGFC	Republican Guard Forces Command
RHAW	Radar Homing and Warning
RMA	Revolution in Military Affairs
RSTA	Reconnaissance, Surveillance, and Target Acquisition
SAM	Surface-to-Air Missile
SIGINT	Signals Intelligence
SINGARS	Single-Channel Ground and Airborne Radio System
SOF	Special Operations Forces
SOP	Standing Operating Procedures
SSM	Surface-to-Surface Missile
TALD	Tactical Air-Launched Decoys
TENCAP	Tactical Exploitation of National Capabilities
TLAM	Tomahawk Land-Attack Missiles
TRADOC	Training and Doctrine Command
UAE	United Arab Emirates
U.N.	United Nations
U.S.	United States

CHAPTER 1

INTRODUCTION

The Battlefield is a scene of constant chaos. The winner will be the one that best controls that chaos, both his own and that of his enemy.¹

Napoleon Bonaparte, The Military Maxims of Napoleon

At 0236 hours, two helicopters launched four air-to-surface missiles at a key early warning site located in a southeastern air defense sector. The attack killed five technicians, injured four, and left three additional people missing. It destroyed the radar and communications equipment at the site, as well as the interface boxes connecting the site's radar to the nation's command and control network. By Defense Ministry estimates, the country would require up to six months to reestablish an effective replacement capability in that portion of the nation (figure 1).²

In the twelve hours following the attack, the nation suffered 135 additional attacks on various targets including the national telephone exchange; various air defense, early warning, and threat acquisition sites; critical communications nodes; airfields; command and control facilities; naval and port facilities; electrical power-generating facilities; and ground forces positioned along the nation's southern border. The nation's capital was without utilities, food, and fuel. It had no capability to observe or report enemy actions in the southern portion of the nation's airspace nor, without resorting to messengers, the capability to command and control air and land forces in the country's southern portion (figure 2).³

Is this the plot of a Tom Clancy thriller? A television movie of the week? On the contrary, these carefully planned and executed attacks on early warning sites and command and control systems initiated the 1991 Gulf War and set the stage for the swift defeat of Iraqi forces. They also raised command and control warfare (C2W) to a new level as a warfighting strategy.

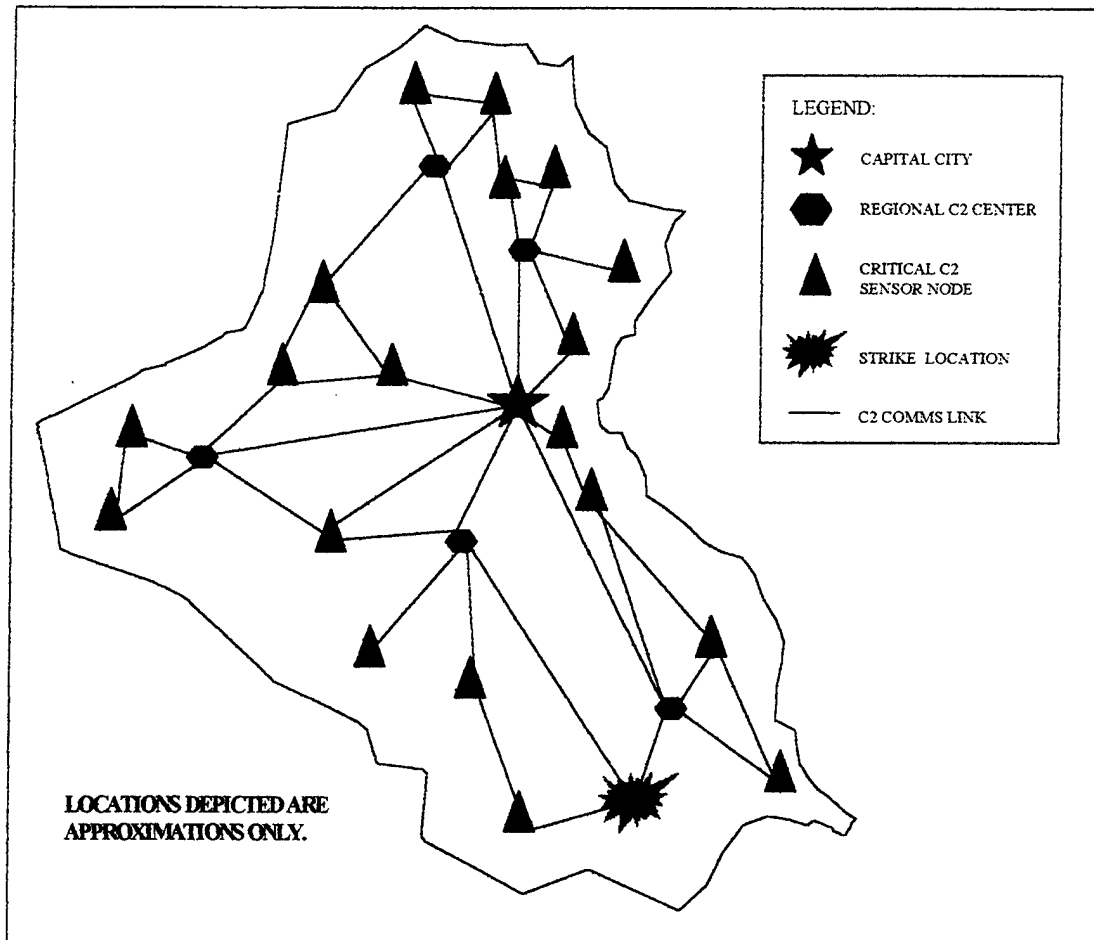


Figure 1. First Strike. Sources: Department of Defense, Conduct of the Persian Gulf Conflict: An Interim Report To Congress (Washington, DC: U.S. Government Printing Office, 1991), 4-18, and Norman B. Hutcherson, Command & Control Warfare: Putting Another Tool in the Warfighter's Data Base (Maxwell Air Force Base, AL: Air University Press, 1994), 3.

The first military objective for Operation Desert Storm, as stated by the Secretary of Defense, was: "Neutralization of the Iraqi national command authority's ability to direct military operations."⁴ For perhaps the first time in a US operation, enemy command and control (C2) was the first and most important goal. The integrated application of C2W against this critical target was key to the remarkable success of the Coalition's efforts against the Iraqis.

The concept of C2W is not new. It has existed in many forms and applications since the very beginning of warfare. The concept of gaining military advantage by disrupting an enemy's ability to

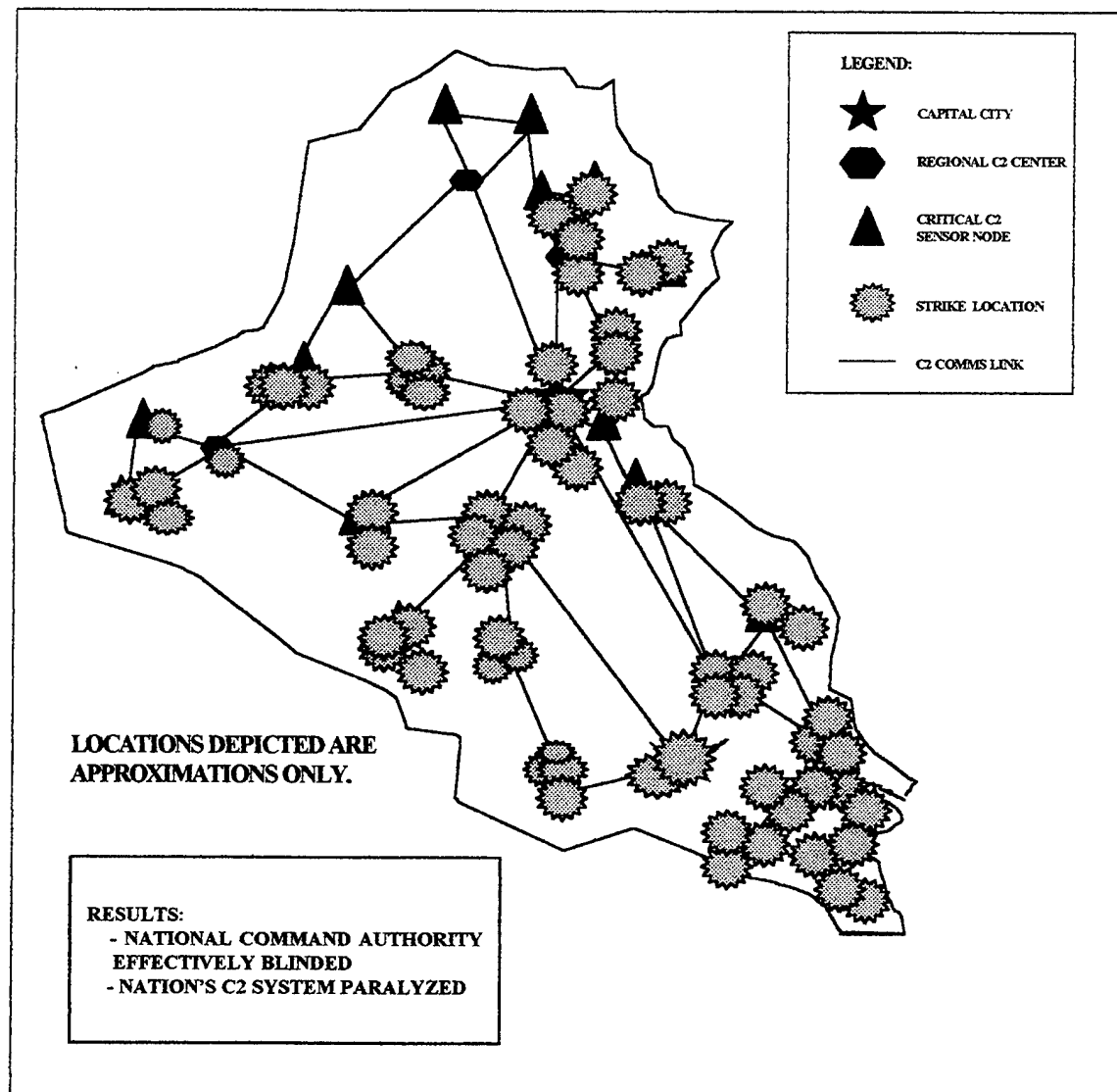


Figure 2. Twelve Hours Later. Sources: Department of Defense, Conduct of the Persian Gulf Conflict: An Interim Report To Congress (Washington, DC: U.S. Government Printing Office, 1991), 4-18, and Norman B. Hutcherson, Command & Control Warfare: Putting Another Tool in the Warfighter's Data Base (Maxwell Air Force Base, AL: Air University Press, 1994), 3.

to command and control his forces is not new. Although the idea has been around for a long time, the Gulf War redefined its application. As a result C2W is emerging as a key strategy, rather than merely a supporting element, in the theater commander's preparation for conflicts both large and small.

The purpose of this thesis is to discuss the newly emerging strategy of C2W and to examine the results on the battlefield when military forces effectively employ it. Chapter 1 will provide a description of the study and discuss the research methodology the thesis will employ, its application to the study, and the conclusions which may be drawn from this particular method. The chapter will include a review of the literature relating to the study topic, including sources already consulted as well as potential supplemental sources which may aid future research efforts.

Chapter 2 will build the foundation for subsequent application and analysis of C2W by outlining the two disciplines which comprise C2W and explaining the five elements they employ. Discussion will focus on how those five tools mutually support each other in forming a C2W strategy. It will also address the critical role intelligence plays in the success of C2W. The chapter will conclude by considering why C2W is important on the battlefield both as a capability and as an overarching strategy.

Chapter 3 will rely on the Persian Gulf War of 1990 to 1991 to demonstrate an application of C2W. Desert Storm is particularly suitable to this purpose for two reasons. First, although the concept of C2W has existed in U.S. military doctrine since the late 1970s, it existed as Command, Control, and Communications Countermeasures (C3CM) and embraced a predominately defensive orientation. During Desert Storm, the Coalition succeeded in bringing together the four elements of C3CM--OPSEC, military deception, physical destruction, and EW--into a single integrated plan that encompassed a much greater offensive focus. In an additional shift from traditional C3CM doctrine, General H. Norman Schwarzkopf, Commander in Chief of the Coalition forces, added the strategy of attacking the entire Iraqi information system, including the human element, by including the fifth element of C2W--psychological operations.⁵ The effectiveness of integrating these five elements into a more offensive strategy contributed to Desert Storm's unprecedented success and was the birth of C2W.

Second, Desert Storm provides a textbook application of C2W strategy. The threatened Marine amphibious landing employed military deception to keep Iraqi coastal defense units in place.

Operations security helped mask the massive shift of Coalition ground forces westward in the historic “left hook.” Physical destruction and electronic warfare combined to disrupt critical communications and noncommunications nodes within the Iraqi C2 system and the associated air defense network. Psychological operations included leaflet drops and radio broadcasts which degraded the morale of Iraqi soldiers and facilitated mass surrenders. The end result was a deaf and blind Iraqi force stripped of the capability to respond with any degree of effectiveness to Coalition actions.⁶

Finally, chapter 4 will integrate the discussion in the previous chapters to provide an overall analysis of the application of C2W during the Gulf War and the import it carries for future operations. It will examine C2W issues arising from the Gulf War and offer recommendations to optimize unit C2W programs.

Hypothesis. C2W is a significant force multiplier when effectively employed on the battlefield.

Significance of the Study. Military forces have always employed various forms of C2W in combat operations. As the U.S. military shifts from the industrial age to the information age, however, its battle focus is changing. It envisions increasingly fluid battles at greater depths and with less “eye-to-eye” contact with enemy forces. It is more reliant on technology and “smart” weapons systems, and less dependant on overwhelming mass. C2W is ideally suited for such an environment. It confuses and paralyzes the enemy, allowing the U.S. to seize the tactical and operational initiative. Likewise, any adversary can employ C2W to disrupt U.S. operations, causing increased casualties and defeat.

With the military’s growing reliance on sophisticated technology in communications and weapons systems, its leadership cannot afford to neglect the capabilities C2W offers. The successful deployment of C2W depends on the emphasis it receives from the commander as well as the ingenuity of the planning staff. It is not successful when the staff hastily throws ill-conceived ideas into plans and operations orders. C2W becomes an effective strategy only when commanders and their staffs

fully understand and integrate it throughout the planning, execution, and termination phases of all operations.

The goal of this thesis is to demonstrate the capabilities of C2W and, in providing an understanding of the application of C2W, to enable the warfighter to effectively increase his combat capability.

Key Terms. The variety of terms used by the military services to discuss C2W can be confusing and misleading. Key definitions applicable to this study are:

Command and Control: C2 is the authority and direction a properly designated commander exercises over assigned or attached forces to accomplish a mission. The commander performs C2 functions through an arrangement of personnel, equipment, communications, computers, facilities, and procedures employed in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission.⁷

Command and Control Warfare: C2W is the integrated use of operations security (OPSEC), military deception, psychological operations (PSYOP), electronic warfare (EW) and physical destruction, mutually supported by intelligence, to deny information to, influence, degrade or destroy adversary C2 capabilities, while protecting friendly C2 capabilities against such actions. C2W applies across the operational continuum and all levels of conflict. Formerly known as Command, Control, and Communications Countermeasures, C2W encompasses both offensive and defensive measures with counter-C2 and C2-protection.⁸

Counter-C2: Actions taken to prevent adversary forces from employing effective C2 by denying information to, influencing, degrading or destroying the adversary C2 system comprise counter-C2.⁹

C2-Protection: Those actions taken to maintain effective C2 of friendly forces comprise C2-protection. They seek to turn to friendly advantage or to negate adversary efforts to deny information to, influence, degrade, or destroy the friendly C2 system.¹⁰

Information Operations (IO): IO includes those military operations, supporting battle command, that enable, enhance, and protect the commander's decision cycle and mission execution, while denying and exploiting the adversary's, to achieve an information advantage across the full range of military operations.¹¹

Information Warfare (IW): IW includes (1) the aggressive use of information means to achieve national objectives, and (2) the sequence of actions undertaken by all sides in a conflict to destroy, degrade, and exploit the information systems of their adversaries. Conversely, information warfare also comprises all the actions aimed at protecting information systems against hostile attempts at destruction, degradation, and exploitation. Information warfare actions take place in all phases of conflict evolution: peace, crisis, escalation, war, de-escalation, and post-conflict periods.¹²

Operational Level of War: This is the level of war at which military leaders plan, conduct and sustain major operations in order to accomplish strategic objectives within theaters or areas of operation. Activities at this level link tactics and strategy by establishing operational objectives, initiating actions, and applying resources to bring about and sustain these events. These activities imply a broader dimension of time or space than do tactics; they ensure the logistic and administrative support of tactical forces and provide the means by which forces can exploit tactical successes to achieve strategic objectives.¹³

Limitations. The decision to limit research to unclassified sources is the major limitation affecting this thesis. While there is sufficient information available from open sources to accomplish the study, more specific detail could enhance chapter 3. The thesis would also benefit from discussions of some of the most recent U.S. operations--information currently limited or unavailable at an unclassified level.

Delimitation. Because the different military services are struggling to define and develop C2W strategies, confusing, sometimes contradictory, theories abound in the field. The indiscriminate use of terms contributes to the confusion and misinformation at every level. Terms such as information warfare, information operations, C2W, intelligence-based warfare (IBW), hacker war,

cyberwar, information economic warfare (IEW), and a plethora of other misused buzzwords abound and often prove counterproductive to the development of C2W thought in the US military.

This thesis will focus on C2W as defined and formulated in joint doctrine, specifically Chairman of the Joint Chiefs of Staff (CJCS), Memorandum of Policy (MOP) 30, Command and Control Warfare, and will avoid service specific concepts. With the doctrine outlined in this publication, chapter 2 will establish a base upon which to discuss and understand the applicable concepts, ideas, and strategies pertinent to discussion in subsequent chapters.

The thesis will further narrow its focus to actions directly on the battlefield or immediately influencing combat operations. It will not venture into a discussion of operations designed to accomplish national objectives, to impact economic systems, to manipulate civilian information systems (except as such actions make a difference in combat operations), or to pursue objectives during times of nonhostilities. The intent of this research is to determine how the effective employment of C2W impacts the battlefield, not to examine the full scope and capabilities of C2W, IW, or IO.

Research Methodology. This study will seek to support its primary hypothesis, that C2W is a significant force multiplier when effectively employed on the battlefield, using a combined historical and comparative approach.

The first step will be to establish a foundation from which to discuss the topic. Using current joint doctrine, chapter 2 will first define C2W then provide an overview of its elements, as well as the concepts for their employment. The objective is to answer the questions: What is C2W? How is it applied? Why is it important?

Building on this foundation, the second step will be to examine how commanders have applied C2W in actual combat operations. Specifically, the thesis will examine the Persian Gulf War of 1990 to 1991, deriving the data for this discussion from historical accounts, service reports, lessons learned, and after-action reports.

The final step will be to compare the doctrinal employment of C2W outlined in chapter 2 with actual battlefield results as presented in chapter 3. Three principle factors, centralized control, intelligence support, and C2W integration, will serve as the basis for analysis. Centralized control is essential to C2W to provide a unity of purpose and to devise a strategy with clear aims and objectives. Accurate intelligence is the foundation of an effective C2W strategy. It highlights key strengths and weaknesses within the adversary's command and control structure, identifies the critical nodes within that structure, and facilitates the employment of C2W assets against the enemy's systems. Finally, C2W does not operate in a vacuum. Its individual elements blend into a mutually supporting effort which in turn supports the commander's overall strategy to achieve maximum effectiveness. These three factors provide a point of departure to examine how C2W affected the Gulf War and if it, in fact, enhanced operations. This analysis will serve to answer the primary research question.

Literature Review. In researching command and control warfare, the available information seemed to fall into three broad categories:

1. Military doctrine, including: CJCS MOP 30 and Joint Publication (Pub) 3-13 which outline joint policy for C2W; Field Manual (FM) 100-6 and Training and Doctrine Command (TRADOC) Pamphlet 525-59 which detail the Army's approach to Information Operations; TRADOC Pamphlet 525-5 which discusses the Army's vision of future joint operations, including Information Operations; and the student text developed by the Armed Forces Staff College to teach the fundamentals of C2W in the Joint C2W Staff Officer Course.

2. Military theorists, presenting their particular philosophy on the subject. This group includes such diverse opinions as the "futurists," who seem to focus largely on "cyberwar" with its more radical applications of information warfare, and the skeptics who question the necessity of C2W altogether as well as the ability of the military to even conduct information warfare. These two groups represent a conflict between those who view "information manipulation"¹⁴ as a revolution in military affairs and those who regard it as simply a passing fad, an effective buzzword in the perpetual

grapple for defense dollars. In the middle is a more pragmatic group which concentrates on the immediate and concrete application of C2W to augment battlefield strategy.

3. Historical accounts, including after action reports and lessons learned, discussing past military operations and their employment of C2W.

This review will examine each of these categories.

Military doctrine. Information warfare is clearly a hot topic in the Pentagon, unavoidable in any contemplation of the future of warfare. Yet the military, the joint world as well as the separate services, seems to have encountered a fundamental difficulty in coming to terms with the subject. Efforts resemble something like the seven blind men coming to grips with the elephant—he who touched its leg called it a tree; he who touched its trunk called it a snake, and so on. A similar process has encompassed the idea of information manipulation. Consider the plethora of terms associated with the topic: information warfare, information operations, intelligence-based warfare, information-based warfare, command and control warfare, cyberwar, etc. To further confuse the process, each term may embrace an entirely different concept depending on the service using it.

For example, joint doctrine views information warfare as a highly classified national policy level strategy, a means to manipulate information to achieve national objectives. Therefore, from a joint perspective, the military does not conduct information warfare. Instead, it employs C2W to implement IW on the battlefield, focusing on the synergistic employment of OPSEC, PSYOP, deception, EW, and destruction to manipulate the adversary's C2 capabilities while protecting friendly C2.

Army doctrine views this approach as too narrow in scope. It embraces a concept it terms Information Operations, a concept which centers on attaining and maintaining information dominance through complete situational awareness and expanded vision while denying the enemy that capability. It emphasizes C2W, information systems, and intelligence as the primary elements of IO and concentrates on setting conditions that allow the friendly commander to operate inside the opponent's decision cycle. Army doctrine focuses on corps and division operations. Although its concept of IO

embraces the global information environment and acknowledges the impact IW may have at the strategic level of warfare, its application of IO focuses primarily on enhancing the capabilities of corps and divisions at the operational and tactical levels of warfare through C2W and assured information connectivity.¹⁵

Likewise, the Air Force grapples with its approach to the subject. It embraces the term "Information Warfare" from a strategic perspective, employing it as a means to accomplish the operational commander's campaign objectives. It views the current focus of C2W as too narrow. From the Air Force's perspective, C2 dominance depends on the attainment of information superiority; targeting the enemy's C2 structure is but one means of attaining that goal. Other targets, not normally considered C2 related, may also be vulnerable to IW techniques and help achieve information superiority. By strategically applying IW against an opponent's informational centers of gravity, his will and capacity to wage war can be neutralized, regardless of the enemy commander's ability to command and control his forces.¹⁶

Navy doctrine centers on the belief that it will be the force employed in the early stages of a crisis to set the conditions for any future conflict. Its focus recognizes the strategic implications of IW as an enabling function to deter conflict or to establish conditions favorable for joint force operations. Although C2W has long been an integral part of Naval operations, its primary application has been C2-protection, in particular the use of deception in maritime operations. The Navy is seeking to expand that perspective in recognition of its ability to shape the battlespace inland. It is striving to obtain the capabilities to use IW to set the conditions for quick, decisive victory. Like the Air Force, the Navy resists limiting the military application of IW to C2 target sets, believing instead that IW techniques can be applied to a wide variety of targets--some beyond the scope of traditional C2W target sets.¹⁷

The Marine Corps, the traditional crisis response force employed to stabilize emerging situations and allow the introduction of follow-on forces, regards C2W as a coordinating strategy at the operational and tactical levels of warfare. C2W's purpose, from the Corps' perspective, is to

enhance the effectiveness of combat operations; its doctrine does not envision the employment of “IW warriors” in a strategic sense. It views C2W as an enabling strategy that leverages the ability of friendly forces to decisively defeat an adversary. Emerging technologies and capabilities in the area of IW must be integrated into the existing constructs of C2W and fine tuned to contribute to the overall C2W effort.¹⁸

The point in providing these service perspectives is to highlight the confusion surrounding IW, IO, and C2W. Services employ similar terminology to define widely different concepts; they employ diverse terminology to explain similar concepts; and each has its own perspective on how best to implement those concepts. Each approach has its merits as well as its drawbacks, although that is a discussion which exceeds the scope of this thesis. The confusion arises when each service comes to the joint battlefield with conflicting theories, doctrine and terminology. Ideally, as the concept of information manipulation--IW, IO, C2W (or whatever it is eventually labeled)--matures, it will develop a common footing across the services and shed the confusion which now exists.

Military theorists. Military theorists take as diverse an approach to information warfare as do the services. Futurists, such as Alvin and Heidi Toffler and Winn Schwartau, see the world on the brink of a revolution in modern warfare. The Tofflers describe how forms of war have changed throughout history; the agrarian age provided the hoe and the sword; the industrial age brought mass production and mass destruction. Tomorrow, as information and knowledge become the core of advanced economies, they believe the world will see the triumph of “software over steel.” Just as the theories of military strategist Carl von Clausewitz foreshadowed the industrialized war of the past two centuries--the bloodiest form of war ever--the Tofflers lay the basis for the “knowledge strategies” they postulate will increasingly dominate military thinking. Schwartau believes the information war has already begun. Modern society is based on access to information--information that moves at the speed of light, is intangible, and is of immense value. Today’s information is the equivalent of yesterday’s factories, yet considerably more vulnerable. Computers and other communications and

information systems are superb first-strike targets. Until the U.S. realizes that information is a vital national asset, Schwartau describes its information systems as a Pearl Harbor waiting to happen.¹⁹

The body of "futurists" works include: War and Anti-War: Survival at the Dawn of the 21st Century, Alvin and Heidi Toffler; Information Warfare: Chaos on the Electronic Superhighway, Winn Schwartau; "Onward Cyber Soldiers," Douglas Waller Washington; and "The Crisis and Opportunity of Information War," Major Kevin B. Smith.

The futurists are countered by a more skeptical group of theorists who views information warfare as a revolutionary new strategy which can enhance the effectiveness of existing forces and weapons but cautions against rushing precipitously to embrace what it describes as a relatively new, poorly understood, and controversial strategy. Information dominance, the group avows, has overwhelming visceral appeal as a war-winning strategy because it elicits visions of an inexpensive, decisive, and relatively bloodless approach to conflict. At the same time, it is impeded by a lack of common definitions, joint and combined doctrine, and guiding principles. It makes a disquieting presumption of unimpeded access to outer space, on assured dominance of the electromagnetic spectrum, and on the absolute infallibility of software-intensive military planning and decision aids. It presumes that the United States can dominate absolutely both outer space and the electromagnetic spectrum, all the while shielding its systems from similar devastation. The skeptics warn of the folly of assuming that any one side can ever dominate all aspects of information warfare and suggest instead that the military's efforts should concentrate on reducing its own vulnerabilities rather than seeking those of its adversaries.²⁰ This more skeptical approach comes from such works as: "What is Information Warfare?", Martin C. Libicki; "Rush to Information-Based Warfare Gambles with National Security," Colonel Alan D. Campen (Retired); and "Information Warfare in 2015," Commander George F. Kraus (Retired).

A third group adopts a more balanced perspective, avoiding the lure of fantasizing a futuristic cyberwar to focus on the somewhat less sensational application of information manipulation to effectively support the needs of the commander on the battlefield. While they acknowledge the

greater implications of IW and IO, they insist that its greatest value will be derived by thoroughly understanding how to effectively employ C2W on the battlefield.

The third group is represented by such works as: Command & Control Warfare: Putting Another Tool in the War-Fighter's Data Base, Lieutenant Colonel Norman B. Hutcherson; "Turning Lessons Learned into Policy," Colonel Jim Gray; "Russian Views on Electronic Signals and Information Warfare," Mary C. FitzGerald; "The Automated Battle: A Feasible Dream?" Colonel José Carlos Albano do Amarante; "C2 Warfare in FM 100-6," Kerry A. Blount and Lauren D. Kohn; "What is Command and Control Warfare?" Lieutenant Commander Dan Strubel; and "The Information and Intelligence Revolution," Colonel Richard F. Riccardelli.

Historical reports. Library shelves abound with volumes analyzing operations in past wars, especially World War II. Although pre-1990 accounts do not label the strategy discussed with the present term "C2W," clearly some of the greatest battlefield victories of military forces worldwide owe their success to the effective application of its principles.

A body of work is gradually emerging at an unclassified level providing analysis of more recent contingencies, such as Desert Storm, Haiti, Somalia, Panama, and Grenada. These accounts further chronicle the benefits of effectively employing C2W and offer insights to avoid misapplication of its concepts. Together, the historical analyses, after-action reviews, and lessons learned offer irrefutable evidence that C2W has broad application in a variety of situations and circumstances, and can significantly alter the course of a battle, and, indeed, a war.

Some of the works germane to this thesis include: Overlord: D-Day and the Battle for Normandy, Max Hastings; "Operation Fortitude: The Backbone of Deception," Major James R. Koch; Conduct of the Persian Gulf War: Final Report to Congress, Department of Defense; From Shield to Storm, James F. Dunnigan and Austin Bay; Military Lessons of the Gulf War, Bruce W. Watson, Bruce George, Peter Tsouras, and B. L. Cyr; "Command and Control Warfare in Forced Entry Operations," Major Robert D. Grymes; "Information Technology in Desert Storm," Major Michael R. Macedonia; and Operation Just Cause, Margaret Roth, Thomas Donnelly, Caleb Baker.

Summary

Chapter 1 has introduced the thesis topic, outlined the research methodology, and reviewed the related literature. The limitations and delimitations described will serve to guide the scope and focus of the study. The historical and comparative research method will serve to validate or disprove the overall hypothesis in a comprehensive and convincing manner. Finally, there is adequate information at the unclassified level to conduct the research and reach a reliable and objective conclusion regarding the topic.

Endnotes

¹Akerly J. Burnod, ed., Military Maxims of Napoleon (New York, NY: Wiley and Putnam, 1845), 17.

²Norman B. Hutcherson, Command & Control Warfare: Putting Another Tool in the Warfighter's Data Base (Maxwell Air Force Base, AL: Air University Press, 1994), 1.

³Hutcherson, 1.

⁴National Defense University, Joint Command and Control Warfare Staff Officer Course: Student Text (Norfolk, VA: Armed Forces Staff College, draft, undated), 1-2.

⁵Hutcherson, 4.

⁶Ibid.

⁷Chairman, Joint Chiefs of Staff, MOP 30, Command and Control Warfare (Washington, DC: U.S. Government Printing Office, 1993), 1-2.

⁸MOP 30, 2.

⁹MOP 30, 2.

¹⁰MOP 30, 2-3.

¹¹Headquarters, Department of the Army, FM 100-5, Operations (Washington, DC: U.S. Government Printing Office, 1993), Glossary-8.

¹²School of Information Warfare and Strategy, Information Resources Management College, Definitions for the Discipline of Information Warfare and Strategy (Washington, DC: National Defense University, 1994-5), 31.

¹³School of Information Warfare and Strategy, 51.

¹⁴This term is adopted solely to facilitate discussion of the literature reviewed. Because of the confusion in terminology which abounds, it is intended to encompass the variety of concepts described in the preceding paragraphs, such as IW, IO, C2W, intelligence-based warfare, information-based warfare, and cyberwar.

¹⁵John Wallace and Jim Jones, "Information Warfare/Information Operations (IO/IW) Update," The Air Land Sea Bulletin no. 96-1 (April 1996): 15.

¹⁶Ibid., 16.

¹⁷Ibid.

¹⁸Ibid.

¹⁹Winn Schwartau, Information Warfare: Chaos on the Electronic Superhighway (New York, NY: Thunder's Mouth Press, 1994), 12-19.

²⁰Alan D. Campen, "Rush to Information-Based Warfare Gambles With National Security," Signal, July 1995, 67-69.

CHAPTER 2

WHAT IS C2W?

In order to win victory we must try our best to seal the eyes and the ears of the enemy, making him blind and deaf, and to create confusion in the minds of the enemy commanders, driving them insane.¹

Mao Tse-Tung, On Protracted Wars

C2W is not a new idea. Military forces have exercised the concept for as long as humans have waged war. The objective of C2W, destroying an adversary's ability to effectively command and control his forces, has always been a lucrative military goal. Likewise, the effort to protect friendly C2 has historically proven to be just as important to successful military operations. Nor is C2W specific to any technology. While it is true that C2W's increasing importance is a direct result of advances in technology, many of its principles have been practiced to a lesser degree throughout human history.

The Mongol armies of the twelfth and thirteenth centuries provide an excellent example of C2W in action. Their fame is associated with their ability to subdue forces several times their size--a feat they accomplished on numerous occasions by waging a form of C2W aimed at "decapitating" their enemies and attacking their "centers of gravity." Employing a network of fast horsemen known as "arrow riders," the Mongols were able to keep distant commanders constantly apprised of situations. Thus, each Mongol leader had timely situational awareness of a vast region surrounding his position. To prevent enemy commanders from enjoying a similar advantage, the Mongols aggressively targeted enemy messengers, often totally eliminating communications between elements of the enemy forces. Typically, enemy commanders regarded no news as good news and blindly continued on oblivious to impending threats. With this strategy, the Mongols typically bypassed the

larger enemy masses and attacked the enemy capital. Frequently, the enemy leader, having no knowledge of the approaching Mongols until they were upon him, fled the capital, leaving the city open and his army without a commander.²

The first modern elements of C2W manifested in the Civil War with the first tactical use of the telegraph to provide information and convey orders. A vast number of Union forces were dedicated to protecting these critical lines of communication before the war's end. In World War II elements of C2W appeared in the use of cryptography, radar and propaganda, and in the deception plan concealing the Allied invasion at Normandy. Vietnam saw the first use of satellite communications and tactical computers and vividly demonstrated the importance of PSYOP, when the loss of public support contributed to the defeat of a technologically superior force. The Persian Gulf War brought C2W into sharp focus with its synergistic application of the elements of C2W. By the launch of the ground war, Iraqi President Saddam Hussein no longer knew the location of his armies, much less the location of Coalition forces. U.S. involvement in Somalia provided additional proof that C2W can be successfully employed by small organizations with limited finances against much larger, well-financed opponents. Aideed ultimately obtained success in part by employing his intelligence forces in small, highly mobile cells. They used cellular telephones and clever tricks, such as bouncing signals off of city walls to foil U.S. attempts to pinpoint sources. He set up an ambush of U.S. troops which was naturally televised via the Cable News Network (CNN) into every American home. This PSYOP strategy, which included televised images of dead Americans being dragged through the streets, succeeded in eliminating most public support for U.S. involvement in Somalia. Soon afterwards, the U.S. pulled out.³

Although the idea of C2W has been around for some time, the exponential growth in technology over the past several decades has significantly increased its relevance and importance. Desert Storm amply demonstrates this. The phenomenal success of C2W against the Iraqi military demonstrated its relevance and effectiveness to military forces worldwide. As a result, U.S. military leaders have analyzed lessons learned, revised policy and doctrine, and shifted emphasis from the

somewhat passive philosophy of C3CM to the more aggressive, offensive-oriented strategy of C2W. Commanders at all levels are becoming more active in the application of C2W as a key element in preparation for conflicts both large and small. In short, although C2W is not new, the way military forces employ it on the battlefield has taken on a new focus and emphasis.

A key factor for the great impact of C2W on the battlefield is that its precepts are applicable at every level of war and across the operational continuum. Each of its five elements--operations security, military deception, psychological operations, electronic warfare, and physical destruction--applies to any contingency or major conflict situation. The commander can employ many aspects of these C2W tools, either individually or collectively, at the strategic, operational, and tactical levels of conflict or war. By incorporating and applying them as a strategy, he can shape his forces and capabilities to meet the enemy in combat under advantageous conditions. This ability to shape the battlefield to achieve an advantage is the essence of strategy and explains the importance of incorporating command and control warfare concepts and ideas into the nation's military strategy.⁴

To set the stage for further discussion, this thesis will first take a more in-depth look at the concept of C2W, its structure, and the elements it employs to achieve its strategic effects. C2W, as defined by CJCS MOP 30 (see chapter 1), is a supporting strategy incorporated into a theater war fighting strategy. It does not stand alone but rather augments operational plans to enhance the chances of success on the battlefield. In short, it is a force multiplier. C2W breaks into two disciplines: counter-C2 and C2-protect. The two work synergistically to degrade enemy C2 and simultaneously protect friendly C2. Both disciplines incorporate the five elements of C2W--OPSEC, deception, PSYOP, EW, and destruction--to target or to protect C2 nodes.

C2 Nodes

A C2 system is an organization of personnel, using specific equipment, following certain procedures to accomplish something within that system. The point where the people, equipment, and procedures come together to do that forms a C2 node. A group of nodes forms a system. To attack

a system, the C2W planner must understand how the nodes within that system fit together to make the system work.⁵

Within a C2 system, one or more nodes may be of such importance that their destruction immediately degrades the functioning of the entire system. C2W seeks to degrade these critical nodes of an adversary's C2 system while protecting those of friendly forces. To provide a viable target, a node must not only be critical to the system, it must also be vulnerable. That is, it must be susceptible to degradation or have an exploitable weakness; it must be accessible or provide some way to reach it; and it must be feasible to degrade the node. Optimally, the C2W planners target nodes that are both critical and vulnerable. Many times, the avenue of vulnerability to a critical node is through the linked nodes within the system.⁶ For example, a critical communications node in a hardened, underground facility may not be readily accessible to attack; however, by striking associated repeater sites, the C2W planner can still isolate the node and effectively cripple the system.

Counter-C2

All military forces employ some type of command and control, normally dependant on communications, to accomplish their missions. C2 is not simply a communications means; it is a system--of personnel, equipment, facilities, communications, and procedures working together to enable the enemy commander to accomplish his mission. The enemy's perceptions, decisions, and reactions are critical elements within this system. C2 is also functional in that many C2 systems coexist on the battlefield. Examples include maneuver control, air defense, logistics, intelligence, in short, virtually any system with an organization and communications structure designed to enable a decision-maker to support combat operations.⁷

Counter-C2 seeks to disrupt this process. To achieve such a goal, two considerations are key. First, the C2W planner must fully understand the unit's mission, the commander's intent, and the concept of operations. Counter-C2 actions can then augment the commander's plan and make it work better. By itself, C2W is meaningless; it has value only when it supports the commander's objectives. Second, the planner must realize that the effects of C2W are relatively short term. That is, counter-C2

directs an action against a specific target for a certain duration of time. Outside that time frame, the enemy will be able to reconstitute his C2 to some degree or to employ viable alternatives. Therefore, he must use C2W at the time and place that will catch the enemy at the greatest disadvantage and at the same time enhance his commander's plans.

When effectively employed, counter-C2 forces the enemy to be reactive. It does this in several ways. First, it slows his tempo by generating hesitation, confusion, and misdirection within his decision making. It essentially disrupts his initiative. As his decision-making process becomes increasingly reactive, his C2 becomes more inefficient and ineffective. Second, it disrupts his operations and planning process. By manipulating the adversary's perception of events, friendly forces can achieve surprise and force the enemy commander into a situation for which he is poorly prepared. Counter-C2 disrupts and misdirects his planning cycle forcing him into a reactive mode. It hampers his ability to conduct effective operations and decreases his battlefield effectiveness. Third, effective counter-C2 disrupts the enemy commander's ability to generate combat power. By presenting a false reality of the battlefield, counter-C2 induces the opposing leadership to generate combat power at the wrong time and place. Fourth, it degrades the enemy commander's decision cycle. This is the logical result of the first three actions. When the enemy does not clearly see the battlefield, he plans poorly and makes incorrect, reactive decisions.⁸ When effectively employed, counter-C2 achieves four basic effects. It denies information to the enemy, influences his decisions, degrades his C2, or destroys his C2 altogether.

First, counter-C2 denies information to the enemy commander by disrupting his observation, degrading his orientation, and interrupting his decision formulation. OPSEC is the key C2W element for hiding vital information from opposing forces. PSYOP and deception augment the effort by influencing the enemy in such a way that he will not look for the vital truths that friendly forces seek to hide. If the enemy's focus is manipulated away from the truth, he may overlook it. Through jamming, communications security (COMSEC), and other associated security disciplines, EW plays

its vital role in concealing information. Finally, destruction can ensure denial of information by removing the physical assets employed by the enemy to obtain information.⁹

Second, counter-C2 manipulates the perception of the enemy commander causing the disorientation of his decision cycle. It allows the enemy to observe a false reality, while hiding vital truth. Through an understanding of the enemy's doctrine, procedures, and C2, it constructs that false reality to lead the enemy to an incorrect and predictable orientation. Counter-C2 induces him to make faulty or delayed decisions and to take inappropriate actions. Deception is the linchpin of perception manipulation. OPSEC is also key because it is the starting point for the deception story. That is, it focuses on what truth the enemy must not know. EW provides an additional tool to the perception manipulation planner, helping to ensure adequate denial of information. Destruction also plays its part by removing the enemy's means of seeing accurate reality.¹⁰

Counter-C2 works to degrade the enemy's C2 primarily by disrupting the connection between the decision maker and the subordinates who translate his decisions into action. EW is the crucial tool for degrading C2 links at key points in time. Destruction severs those links on a more permanent basis. C2W planners must consider, however, the impact that degradation may have upon ongoing efforts to influence. The enemy commander must be able to translate his decisions (those the C2W strategy has influenced so as to be flawed) into action. Severe degradation of his decision/action command, control, and communications (C3) link may negate that influence. The risk then arises that enemy subordinate commanders will make their own decisions and take independent actions--ones friendly forces cannot predict or control.¹¹

The last effect, destruction, is the most difficult to achieve. It requires friendly forces to dedicate sufficient resources to achieve lasting destruction. To some extent, this will necessitate precision-guided munitions and stealth technology. Like degradation, destruction may negate other C2W effects, such as influencing, because of its damage to the enemy's observation and orientation capabilities.¹²

An additional factor comes into play when C2W planners seek to achieve any of the effects described above. The ability to accurately locate a C2 node will have a bearing on the friendly attack strategy. Obviously, an aircraft must have pinpoint accuracy to drop a laser-guided bomb on an enemy node; however, the planner does not require the exact location of an enemy commander to employ PSYOP or deception.¹³

C2-Protect

By employing effective counter-C2, friendly force commanders stay ahead of the enemy commander's decision and reaction cycle and maintain the initiative at the expense of the adversary. At the same time, they must ensure that their own forces have adequate C2. They have to protect their own C2 from enemy counter-C2 and from C2 fratricide within the friendly forces.¹⁴

Potential opponents will most likely attempt to employ counter-C2 against friendly forces. Their ability to do so does not depend on their technical sophistication or relative combat power. In fact, in a situation where friendly forces have technical superiority and favorable combat power ratios, counter-C2 may become the enemy commander's primary war fighting strategy. The ability of any force to gain and maintain C2 superiority will depend not only on its effective counter-C2 strategy, but also upon its ability to practice effective C2-protection.¹⁵

Normally, C2-protection is equated with measures taken to ensure an ability to use the electromagnetic spectrum for effective C2. While it certainly encompasses that ability, there is another area that may necessitate more aggressive C2-protection. The friendly force commander makes key decisions as part of effective C2. He bases those decisions upon an assessment of the friendly and enemy situations derived from information and intelligence reports. These decisions become the real interface between "command" and "control." OPSEC can help identify those decisions that are crucial to friendly operations and initiate appropriate measures to minimize the enemy's ability to recognize them and react in a preemptive manner. Equally as important, by developing an understanding of enemy deception and PSYOP capabilities friendly forces can

minimize their own faulty perceptions of enemy intentions and dispositions on which they base key decisions.¹⁶

No matter how thoroughly C2W planners address C2-protection, it is unreasonable to assume that all necessary C2 will work all the time. Even if the enemy is not actively trying to counter friendly C2, events on the battlefield are bound to generate some level of mutual interference, misunderstanding, or fog of war. Optimally C2-protection can minimize disruptions on those systems most crucial to friendly operations. To accomplish such a task C2-protection has three basic principles:

Offensive protection uses the five elements of C2W to reduce the enemy's ability to conduct counter-C2. The enemy's ability is based on the capabilities of his intelligence systems, on his C2 systems for conducting counter-C2, and on his having the tools of C2W. Offensive C2-protection targets those three elements with actions that normally take place on the enemy's side of the forward line of own troops (FLOT). Two of the three elements, intelligence and a C2 system for counter-C2, will be very similar to targets cited in friendly counter-C2 planning. A clear-cut division between counter-C2 and C2-protection does not always exist--nor does it need to.¹⁷

Defensive protection employs appropriate physical, electronic, and intelligence protection means to reduce friendly C2 vulnerabilities to adversary Counter-C2. These actions normally occur on the friendly side of the FLOT.¹⁸

Coordination and deconfliction reduce friendly mutual interference in C2, particularly in the use of the electromagnetic spectrum to support command and control.¹⁹

The effects of C2-protection mirror those of counter-C2. They deny the information the adversary commander needs to take effective action. They influence him to take the wrong action, to take action at the wrong time, or to take no action at all. They degrade or destroy his capabilities to perform counter-C2 against friendly forces.²⁰

In short, the overall focus of C2W is to protect the command and control of friendly forces while at the same time seeking to deny, deceive, disrupt, or, if necessary, destroy the command and

control capabilities of the enemy. Its goal is to get inside the decision-making cycle of the opponent, thus forcing him to lose the initiative and resort to a reactive mode of operation. Prior to the fall of the Berlin Wall and the collapse of communism, allied forces avoided targeting the command and control of enemy forces. To do so, they feared, would result only in an undesirable escalation of hostilities. That belief gave the enemy commander a valuable strategic and tactical advantage. Today, leaders realize that focus was shortsighted. Without effective command and control, enemy commanders must resort to autonomous operations. Although their actions may achieve some degree of success locally, in the long run they will lose the synergistic advantage of units fighting as a coordinated whole. For this reason, friendly force commanders must make the denial, disruption, deception, and if necessary, the destruction of the enemy commander and his deployed C2 structure a primary objective.²¹ The next few pages will examine more closely the five elements of C2W and how, when effectively employed, they can help achieve and exploit that battlefield advantage.

Operations Security

The military's present concept of operations security was born around 1967 during the Vietnam War. U.S. B-52 bomber raids were not achieving the desired results and officials suspected that someone was leaking classified information to the enemy. The ensuing investigation revealed quite a different problem. The enemy was simply accessing the international flight plans filed by the B-52 pilots to obtain the general time of their attacks. Since U.S. forces moved out of the strike zones prior to the arrival of the B-52s, enemy forces could then determine not only the time but also the place of the U.S. attacks. The problem was not the disclosure of classified information but the leakage of unclassified indicators that revealed critical information.²²

OPSEC arose as a process to prevent such leaks, to deny enemy forces information about friendly intentions, capabilities, or limitations. It accomplishes these objectives by identifying which actions enemy collection systems can observe, determining which indicators enemy intelligence can interpret or piece together to ascertain friendly intent, and then developing and employing selected measures to eliminate or reduce friendly vulnerabilities to such actions. It can help conceal friendly

preparations for crises or war, especially when planners combine it with deception, elements of EW, or PSYOP. When correctly employed, OPSEC is an excellent means to achieve strategic or tactical surprise.²³

Through the OPSEC Planning Process, planners first identify critical information, that is, activities or indicators that will reveal friendly intentions or courses of action. When collected and analyzed by enemy intelligence, these elements of critical information reveal friendly plans (for example, the B-52s filing international flight plans to bomb Vietnam). Critical information may include both classified and unclassified data derived from such things as the commander's mission statement, his concept of operations, unit standing operating procedures (SOP), and unit contingency plans. Next, the planners must develop a thorough understanding of an adversary's intelligence capabilities, including his means of collecting information and his ability to analyze and disseminate it. The third step of the process involves comparing the first two. Analysis determines if the enemy has the ability to collect friendly elements of critical information. From there, the commander decides what actions to take to conceal his critical information or, conversely, to accept the risk of doing nothing at all. Then planners recommend the appropriate countermeasures. Since forces cannot conceal an entire operation, they focus on protecting sufficient information to achieve the surprise necessary to ensure the success of their operation.²⁴

During the Persian Gulf War, OPSEC, combined with the other elements of C2W plus an effective air campaign, enabled the allied forces to move more than 270,000 armed troops virtually undetected in preparation for the ground offensive. This forms a sharp contrast to the Vietnam conflict and the critical B-52 information unwittingly provided to the North Vietnamese.²⁵ Table 1 summarizes ways OPSEC supports C2W operations.

Psychological Operations

Psychological operations as described in Joint Publication 3-53, consist of actions designed to convey "selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning and, ultimately, the behavior of foreign governments, organizations,

Table 1. OPSEC Capabilities

OPSEC CAPABILITIES		
Determine Indicators and Vulnerabilities Document and Physical Security Deny Access Apply Information Security Provide Security to Plans and Orders Protect Friendly Decisions Keep Enemy From: Planning Conducting Deception Hardening Employ Counterintelligence	Assess Indicators and Vulnerabilities Camouflage Delay Information Needed to Make Decisions Ensure Surprise Degrade Enemy Decisions Employ Effective Radio Procedures Apply Information Security Employ Counterintelligence	Assess Indicators and Vulnerabilities Deny Enemy Knowledge of: Critical Nodes Friendly Intentions Capabilities Ensure Dispersal Starve Enemy Intelligence Apply Information Security Employ Counterintelligence
NONCOMBAT		COMBAT
PEACETIME	CONFLICT	WAR
Promote Peace	Deter War/Resolve Conflict	Fight and Win

Source: Headquarters, Department of the Army, FM 100-6, Information Operations, Draft , Unedited (Washington, DC: U.S. Government Printing Office, working draft, 1995), 3-9, figure 3-4.

groups, and individuals.” Their purpose is to induce or reinforce attitudes and behavior that facilitate the attainment of friendly objectives. Such operations are a vital part of a broad range of U.S. political, military, economic, and informational activities, and when properly employed, can lower the morale and reduce the efficiency of enemy forces or create dissidence and disaffection within their ranks.²⁶

Psychological operations require extensive intelligence information regarding such things as the location and identity of the target, its vulnerabilities, peculiarities, and susceptibilities, and existing political, military, social, cultural, and historical conditions within the target area. PSYOP employs a variety of actions, such as political and diplomatic communiqués, leaflet drops, loudspeaker broadcasts, and various other means of transmitting information. The PSYOP planner can design operations to gain a strategic advantage or simply to encourage enemy soldiers to defect, desert, flee, or surrender.²⁷

The employment of any element of national power projection, particularly the military element, has a certain psychological dimension. The U.S. strategic deterrent capability relies to a large extent on foreign perceptions of the country's military strength and capabilities. Its ability to effectively accomplish such strategic objectives as power projection, deterrence, etc., hinges on how successfully it influences the perceptions of adversaries as well as allies. Military PSYOP provides a planned, systematic process of conveying messages to, and influencing selected foreign groups. It can be instrumental in establishing and reinforcing foreign perceptions of U.S. military superiority.²⁸

Throughout history, psychological actions have influenced enemy groups and leaders. In modern times, the expansion of mass communications capabilities has greatly extended the reach and the effects of PSYOP. Any nation can multiply the effects of its military capabilities by communicating directly to its enemies the threat of force or retaliation, conditions of surrender, safe passage for defectors, incitations to sabotage, support to resistance groups, and other messages. The effectiveness of such communication depends on the target audience's perception of the communicator's credibility and capability to carry out the actions threatened.²⁹

It is essential that the PSYOP campaign contain enough truth so that it brings a credible message to its audience. PSYOP loses any effectiveness when the enemy does not believe the message. History provides countless examples of psychological campaigns devoid of credibility. Tokyo Rose, Hitler, Hanoi Hannah, Kim Il-Sung, and more recently Saddam Hussein launched psychological operations effective for little more than entertainment purposes. On the other hand, the reactions of enemy leaders to U.S. psychological operations attest to their effectiveness. Traditionally, opponents have jammed PSYOP broadcasts and attempted to isolate their troops from any exposure to them. In World Wars I and II, and as recent as the Persian Gulf War, enemy commanders declared it illegal for their soldiers to possess U.S. PSYOP leaflets.³⁰

In spite of its demonstrated effectiveness, U.S. military emphasis on psychological operations has been sporadic at best. Following the success of General George C. Marshall's Belfort Ruse during World War I, the War Department neglected to appoint any PSYOP point of contact in the

interwar years from 1918 to 1941. Likewise, after the successes of World War II, military interest in PSYOP subsided to the point that U.S. PSYOP capabilities were virtually nonexistent in the 1960s and 1970s. For example, when the Army activated the 6th PSYOP Battalion in 1965 there were not enough PSYOP-trained officers to man the unit. The situation had improved very little by 1981 when President Ronald Reagan took office; the active component was understrength, overcommitted, inadequately trained, and poorly equipped.³¹

After taking office, President Reagan published a national security strategy that emphasized four basic components--including information--as a source of national power. In 1984, as a result of this focus, the President directed the Department of Defense (DOD) to rebuild its PSYOP capability; in 1985, he approved the first DOD PSYOP Master Plan.³²

PSYOP reached a pinnacle during Desert Storm, achieving unexpected and spectacular success against Iraqi forces. The employment of pamphlets and leaflets in conjunction with hard-kill assets such as the BLU-82 offers a vivid example. These 15,000-pound bombs blasted paths through Iraqi ground defenses. PSYOP units integrated pre- and post-drop leaflets to first let the Iraqi soldiers know the bombs were coming, and afterwards, to alert them that the bombs would be back again--and again. The psychological impact on the beleaguered Iraqi troops resulted in overwhelming numbers crossing the lines to surrender.³³ Table 2 summarizes PSYOP's role in C2W operations.

Military Deception

Joint Publication 3-58 defines deception as "those actions executed to deliberately mislead adversary military decision makers as to friendly military capabilities, intentions, and operations, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission."³⁴ Simply stated, deception operations mislead an opponent through the manipulation, distortion, or falsification of friendly dispositions and capabilities. They induce him to act--or fail to act--in a manner prejudicial to his own interests and exploitable by friendly forces.³⁵ Deception operations degrade the accuracy of enemy reconnaissance, surveillance and target acquisition (RSTA), and intelligence gathering resources. They do not generally seek to

Table 2. PSYOP Capabilities

PSYOP CAPABILITIES		
Enhance Perception of Military Capabilities Support CINC/Country Team Objectives Promote Democratization, Professionalization and Human Rights Enhance Counter-Drug Efforts Support Peace Operations Support Nation Assistance and NCA Assist in Natural Disaster Response	Help Deter/Contain Conflict Explain US Goals, Rewards, Consequences Encourage Allied Contributions and Resolve Mobilize Popular Support Communicate Credible US Intent, Capabilities Shape Expectations	Prepare the Battlefield Reduce Combat Power / Effectiveness Increase Impact of US Combat Power Undermine Decision-Making Process Enhance Deception Operations Encourage Allied Contributions Counter Propaganda Shorten Conflict and Save Lives
NONCOMBAT		COMBAT
PEACETIME	CONFLICT	WAR
Promote Peace	Deter War/Resolve Conflict	Fight and Win

Source: Headquarters, Department of the Army, FM 100-6, Information Operations, Draft, Unedited (Washington, DC: U.S. Government Printing Office, 1995), 3-12, figure 3-6.

destroy his intelligence capabilities altogether for they usually require a means to feed him false information. However, deception operations seek to control what the enemy collects in order to induce him to draw wrong conclusions from what he does see.³⁶

Deception operations manipulate perception. The best deception story, one with a greater probability of success, is one that reinforces an adversary's ideas or biases. It seeks to exploit some perception already resident in the enemy's mind. His biases may be cultural, political, doctrinal, or derived from numerous other sources. Deception planners must first identify that bias, or perhaps create one, then play to it with their deception story. Field Marshall Allenby did exactly that at the battle of Megiddo in 1918. He ascertained that the Germans and Turks linked his name with a cavalry thrust against their desert flank. Accordingly, he designed his deception operation to reinforce that belief. Naturally, he attacked elsewhere and won a decisive victory.³⁷

Seven basic principles provide guidance for planning and employing military deception.

Focus. The deception story must target the opponent capable of taking the desired action. The adversary's intelligence system is normally only a conduit to get the desired information to that decision maker; it is not the primary target.³⁸

Objective. The deception operation must cause the adversary to take, or not take, specific actions; its objective is not to make him think but to act.³⁹

Centralized Control. A single element must direct and control the deception operation. This is necessary to avoid confusion, to ensure that the various elements involved in the deception are portraying the same story, and to ensure their actions do not conflict with other operational objectives. That centralized authority may decentralize the execution of the deception plan provided all participating elements remain focused on that single plan.⁴⁰

Security. Successful deception operations require strict security. An opponent must not know of any intent to deceive or be able to discern the execution of that intent. Deception planners apply strict need-to-know criteria to each deception operation and to each aspect of that operation. An active OPSEC effort is essential to deception operations to deny critical information about both actual and deception activities.⁴¹

Timeliness. A deception operation requires careful timing. Planners must provide sufficient time for its portrayal; for the adversary's intelligence system to collect, analyze, and report; for the opponent's decision maker to react; and for the friendly intelligence system to detect the action resulting from his decisions.⁴²

Integration. To enhance success, deception planners cannot operate in a vacuum. They must plan the deception strategy simultaneously with operational planning to insure they fully integrate it with the basic operation they design it to support.⁴³

Economy of Force. The deception operation does not normally constitute the main focus of a campaign. It is usually an economy of force effort and must enhance, not detract, from the main effort.⁴⁴

Because deception operations rely largely on psychological perceptions, they are not as formalized or doctrinally defined as other elements of C2W. Although a good imagination can enhance deception planning, the percepts outlined below provide more concrete principles on which to base deception operations.

It is generally easier to reinforce a preexisting belief than to manufacture evidence to change that belief. Therefore, deception planners should first examine how they can turn an enemy's existing precepts to friendly advantage rather than attempting to change them. One of the most striking demonstrations of this principle was the selection of the invasion site and cover plan for the D-Day invasion at Normandy. Hitler, along with most of his senior military advisors, believed that the Pas de Calais region was the most likely area for the Allied invasion of Europe. Moreover, Allies knew of this belief through intercepts obtained with ULTRA, the top secret espionage and cryptographic breakthrough that enabled the British to read the German codes. The German preconception served as the basis for an elaborate deception plan designed to reinforce their belief. If an opponent perceives what he expects, then his expectations lend greater leverage to the friendly deception plan and its probability of success is greater.⁴⁵

Human information processing offers several limitations which are lucrative exploitation opportunities in the design of deception schemes. One weakness, termed "the law of small numbers," describes the human propensity to draw critical inferences from limited data samples. The Cuban Missile Crisis of 1962 provides an example of this phenomena. The U.S. intelligence community reasoned that since Khrushchev had never put medium- or long-range missiles in any satellite country, he certainly would not station them on an island 9,000 miles away from the Soviet Union, and only 90 miles from the U.S. where they were bound to provoke a sharp American reaction. Unfortunately, this critical deduction was based on a sample size of less than five.⁴⁶

A second limitation in human information processing impacting the deception process is the frequent inability of targets to detect small changes in indicators even if the cumulative change over time is large. For this reason, conditioning or desensitizing is an effective deception technique. The

breakout of the German ships *Scharnhorst*, *Gneisenau*, and *Prinz Eugen* from Brest on February 12, 1942 offers a classic example of this principle. Ordinarily, the jamming operations which facilitated the breakout would have been a significant indication that something was happening. However, the British radar operators dismissed it as the result of atmospheric disturbance. Their error resulted from a carefully orchestrated German ruse in which the Germans jammed the British radar sites every day at the same time to build their belief that the atmosphere was interrupting the receipt of any signals. The British became so accustomed to the atmospheric problems that the ships were able to escape.⁴⁷

A third weakness in human information processing is a trend to dismiss unlikely events as impossible events. Bold and imaginative strategies, such as Hannibal crossing the Alps or the U.S. landing at Inchon, demonstrate adept exploitation of such a fallibility.⁴⁸

In much the same fashion, repeated false alarms desensitize an opponent and enhance the ability of a deception operation to achieve surprise. For example, every year, U.S. military headquarters in Saigon predicted a winter-spring offensive by the North Vietnamese that never materialized. As a result, the warnings issued before the 1968 TET offensive were ignored with disastrous results.⁴⁹

Deception operations become more difficult as the means of gathering information expand. However, within limits, the more avenues feeding the deception story to a target, the greater likelihood he will believe it. When possible, planners should seek to avoid generating ambiguity or uncertainty in the mind of an adversary which could induce him to take actions contrary to friendly plans. Instead, they should seek to make him more certain of a falsehood so that his actions are in concert with their intentions.⁵⁰

The sequencing of deception operations is another important principle. The aim is to portray the false story for as long as possible. Deception planners seek to hide their true intentions until the last feasible moment to deny the adversary an opportunity to effectively react. The Allied surprise at the German attack on Norway demonstrates this principle. Although the Allies detected German ships moving toward Norway, they misinterpreted their mission as an attempt to break the Allied

blockade into the Atlantic. When the true intent manifested, the Allies were unable to take appropriate action and the Germans landed unopposed.⁵¹

A method of ensuring accurate feedback increases the chances that deception operations will be effective. Feedback reveals if an opponent is detecting the story and reacting to it as intended. One of the most dramatic examples of the crucial role of feedback in deception operations was the intelligence provided by ULTRA. The Allies immediately knew Hitler's reactions to their activities and how well they were convincing him of an attack at Pas de Calais. Many credit ULTRA information as the key element in the success of the invasion.⁵²

The examples discussed in the preceding paragraphs are but a token representation of the numerous historical accounts demonstrating the advantages garnered through effective deception operations (see also table 3). Wise military planners have used them throughout history as a low cost and effective means of causing the enemy to waste his efforts.

Table 3. Military Deception Capabilities

MILITARY DECEPTION CAPABILITIES		
Support OPSEC Degrade RSTA Degrade Enemy Intelligence Influence the Enemy Specialized Equipment and Materials	Perception Manipulation Defeat the Mind Paint a False Picture Hide the Real Deceive and Confuse Enemy RSTA Distort Enemy Situation Awareness	Demonstrations Feints Displays Ruses Target Lower Echelons C2-attack Forces Electromagnetic Deception Degrade Enemy C2-attack
NONCOMBAT		COMBAT
PEACETIME	CONFLICT	WAR
Promote Peace	Deter War/Resolve Conflict	Fight and Win

Source: Headquarters, Department of the Army, FM 100-6, Information Operations, Draft, Unedited (Washington, DC: U.S. Government Printing Office, 1995), 3-11, figure 3-5.

Electronic Warfare

A discussion of EW must begin with definitions of several key terms. Electronic warfare is "military action involving the use of electromagnetic or directed energy to control the electromagnetic spectrum."⁵³ It has three basic missions: to attack an opponent's combat capability, to protect friendly combat capability against the undesirable effects of both friendly and enemy employment of EW, and to conduct surveillance of the electromagnetic spectrum for immediate threat recognition in support of EW operations as well as other tactical actions such as threat avoidance, targeting and homing.⁵⁴ Its three subdivisions are electronic attack (EA), electronic protection (EP), and electronic support (ES).

Electronic attack consists of offensive use of the electronic spectrum as well as directed energy to directly attack an opponent's combat capability. It employs such non-destructive actions as jamming and deception to degrade or neutralize enemy systems, but also relies on such destructive assets as anti-radiation missiles (ARM) and directed energy weapons (DEW).⁵⁵

With today's technology, EA brings much more to the battlefield than simply a jammer degrading enemy radio or radar. Electronic deception, for example, employs radiation, re-radiation, alteration, suppression, absorption, denial, enhancement, and reflection of electromagnetic energy to convey misleading information to an enemy as well as to deny valid information to his electronics-dependent weapons. It employs expendable antennas to simulate radar dishes, attracting ARM attacks away from real radar sites. Likewise it can purposely feed deceptive information to the adversary's signals intelligence (SIGINT) collection systems in support of operational or strategic deception. Electronic deception operates across all points of the spectrum of conflict.⁵⁶

Likewise, the recent development of destructive capabilities adds a new dimension to EW. In the past, EW's only destruction means consisted of using SIGINT to find an opponent's electronic equipment then directing artillery or aircraft to strike it. Today, technology has greatly expanded the capability to turn the electromagnetic spectrum against a foe. For example, ARMs, consisting of a seeker head on a high explosive missile, can detect a certain type of radar transmission then follow

its radar waves back to their source. DEWs, such as lasers, add a significant ability to identify and range targets. And finally, EA can employ such things as electromagnetic pulse (EMP) bursts to destroy an enemy's electronic gear.⁵⁷

Electronic protection is the defensive side of EW, protecting friendly forces against both an enemy's use of the electromagnetic spectrum and undesirable effects of friendly use. It essentially encompasses two efforts: preventive measures employed to identify and correct potential problems, and remedial measures used to identify and correct actual problems. Spectrum management, including both frequency management and frequency deconfliction, offers a vehicle to accomplish much of the EP mission.

Electronic support focuses on those actions taken "to search for, intercept, identify, and locate sources of radiated electromagnetic energy for the purpose of near-real-time threat recognition."⁵⁸ It assists the operational commander to make immediate decisions involving EA, EP, avoidance, targeting, or other tactical employments of force. During Desert Shield, US EP-3 and RC-135 aircraft monitored Iraqi radar and communications networks to identify critical C2 nodes. Their successful collection of Iraqi emissions led to an exemplary counter-C2 campaign and the devastation of Saddam's C2 network.⁵⁹

Prior to Desert Storm, EW was the primary soft-kill option of C2W. Its focus on electronically jamming an opponent's communications and electronic sensors effectively disrupted the Iraqi command and control system and prevented it from gathering critical information or transmitting command decisions. With the addition of hard-kill capabilities, EW has become much more offensive. Its mission has expanded beyond self-protection or defensive jamming on ingressing aircraft. Today, EW works with the other elements of C2W to introduce delays into the enemy's decision-making cycle and to decrease the reliability of the information enemy intelligence assets are able to collect. It degrades the enemy commander's ability to accurately perceive the situation on the battlefield and react to it appropriately.⁶⁰ Because of the dependence virtually every military force

has upon the electromagnetic spectrum, EW can provide significant advantages to the combatant who effectively employs it (table 4).

Table 4. Electronic Warfare Capabilities

ELECTRONIC WARFARE CAPABILITIES		
Monitor Early Warning Locate Critical Nodes Find Targets Protect Personnel, Equipment and Facilities	Deny Intelligence Disrupt RSTA Deconfliction Reduce Signature Degrade Decision Making Jam/Deceive Electronic Battle Damage Assessment Electronic Protection and Survivability	Spectrum Supremacy Attack Entire Electromagnetic Spectrum Synchronize Jamming and Exploitation Jam Enemy C2-attack Destroy Enemy Sensors and Target Acquisition Delude and Deceive Minimize Collateral Damage Point and Wide Area Targets Electronic BDA Electronic Protection and Survivability
NONCOMBAT		COMBAT
PEACETIME	CONFLICT	WAR
Promote Peace	Deter War/Resolve Conflict	Fight and Win

Source: Headquarters, Department of the Army, FM 100-6, Information Operations, Draft, Unedited (Washington, DC: U.S. Government Printing Office, 1995), 3-7, figure 3-3.

Destruction

For the purposes of C2W, destruction of a C2 ability means that function cannot perform either permanently or for a given period of time. In terms of destroying a piece of equipment, military unit, or facility, the following three categories apply. Historically, an element is considered destroyed when actions incapacitate at least 30 percent of its personnel, equipment, or functionality. If they affect only 10 to 30 percent, they have neutralized the element. Actions suppress the element when they achieve a casualty rate between zero and 10 percent of its personnel, equipment, or

functionality. Suppression temporarily stops a unit from performing its primary function, and is generally achieved without inflicting casualties.⁶¹

Since the C2W strategy generally cannot achieve total destruction of enemy C2 nodes, nor does it have unlimited access to destruction assets, the C2W planner must carefully program efficient and effective destruction support to C2W. The four-step destruction process offers a guide to accomplish this.

Know unit plans. Effective C2W planning is impossible without a thorough understanding of the unit combat plans. The commander's mission and intent statements are key indicators of how he envisions accomplishing the mission and serve as the basis for a complementary C2W plan. From these combat plans the C2W planner first ascertains the units involved in the operation, the assets and weapon systems available for destruction, and the capabilities and vulnerabilities of those systems. Next he determines the critical decision points in the operation. This will pinpoint when operations can most effectively disrupt or destroy an opponent's C2 as well as when it is essential to protect friendly C2.⁶²

Know the enemy. Knowledge of the adversary's key leadership, both military and political, including descriptions of the leaders' personalities and backgrounds often provides valuable clues on the methods and techniques of C2 they prefer as well as the equipment on which they habitually rely. Knowledge of the enemy's C2 structure enables the C2W planner to identify his critical nodes--those elements, positions, or communications entities whose disruption or destruction immediately degrades an enemy's ability to effectively command, control, or conduct combat operations. Since operations cannot expect to destroy all enemy communications nodes, the C2W planner seeks to strike those which most significantly degrade enemy C2.⁶³

Target nomination. The C2W planner relies on the preceding two steps to accomplish effective target nomination. The information developed enables him to establish the importance of a target, its exact location, the time frame for its destruction, what level of destruction it requires, as well as a general idea of who will destroy it and how they will accomplish the mission. His

participation at joint targeting boards is essential if C2W missions are to receive any priority for destruction among many competing demands.⁶⁴

Destruction Feedback. Feedback on the effects of these destruction efforts takes a variety of forms, with battle damage assessment (BDA) as the most common. A function of the intelligence staff, BDA relies heavily on overhead imagery and aircraft gun cameras. It works effectively with visible targets, such as aircraft on a runway, but becomes more subjective with hidden targets, such as underground command posts. Often, intelligence efforts can determine some degree of damage only when a target node ceases to transmit or enemy forces are unable to react on the battlefield.⁶⁵

Destruction in support of C2-protection involves eliminating the enemy's means of affecting friendly C2. It requires targeting units, weapons systems, reconnaissance elements, and intelligence collection sites, and follows the same basic four-step process outlined above. The C2W planner must first know his unit's plans, specifically when and where C2 is most vulnerable to enemy action. He must determine the opponent's ability to affect friendly C2, his ability to employ such things as reconnaissance systems, jammers, and other intelligence collection assets, as well as his capability to conduct deep operations and terrorist actions. With that information, he seeks to strike targets which will effectively negate an opponent's ability to interrupt friendly C2. The degree to which the enemy is unable to reach friendly C2 is an indication of the success of his C2-protection efforts.⁶⁶

For destruction purposes, there is no "C2W" weapons system; basically, any weapon can target C2. Widely speaking, destruction capability consists of land, sea, and air forces. Land forces include primarily artillery, special operations forces (SOF), and surface-to-air missiles (SAM). Artillery is most effective against area and unprotected targets, but has little utility against protected, underground facilities. SOF form a very effective C2W force. However, they require extensive planning, a means of insertion, as well as a method of extraction. They are often most valuable when employed to locate critical C2 nodes that other systems will then destroy. SAM systems frequently perform a C2-protection role. They defend against enemy aircraft and missiles targeting rear areas. Sea forces offer naval gunfire and long-range, sea-launched missiles--both excellent C2W systems.

Hydrography and range restrict naval gunfire, whereas their limited numbers and high cost constrain missile use. Missiles, however, are extremely accurate and capable of very long ranges. Air assets, including helicopters, form the mainstay of C2W destruction. Their inherent speed, range, and flexibility give them access to any part of the battlefield. Recent advances in guided munitions add a relatively low cost, precise, and lethal means of destroying even hardened, underground facilities. Their main limitation is their requirement for air superiority during attacks to prevent unacceptable losses of the high-value platforms.⁶⁷

To summarize, physical destruction requires the ability to identify, locate, and prioritize enemy targets accurately and then to destroy them selectively (table 5). Physical destruction may

Table 5. Physical Destruction Capabilities

PHYSICAL DESTRUCTION CAPABILITIES		
Identify Targets Determine Feasibility of Attack Plan Redundancy Damage Control	Neutralize or Degrade Risk vs Benefit Ratio Protect Friendly Critical Nodes Attack Enemy Critical Nodes	Degrade or Destroy Attack Enemy Critical Nodes Attack CPs and other Point Targets Attack Area Targets Harass and Interdict Timing is Everything Limited Long Term Effects
NONCOMBAT		COMBAT
PEACETIME	CONFLICT	WAR
Promote Peace	Deter War/Resolve Conflict	Fight and Win

Source: Headquarters, Department of the Army, FM 100-6, Information Operations, Draft, Unedited (Washington, DC: U.S. Government Printing Office, 1995), 3-5, figure 3-2.

seem the best method to deny command and control to the enemy but it can also be an unnecessary waste of critical resources.⁶⁸ C2W is a strategy of options. The C2W planning process must first determine whether or not destruction is the best option. Sometimes disruptive means, such as jamming, can achieve the results where and when desired yet leave C2 nodes intact for exploitation

by PSYOP or deception elements and reserve limited destructive resources for targets where physical destruction is the only option.

Intelligence

No discussion of C2W is complete without emphasis on the critical role played by intelligence. In order for any C2W plan to be successful, accurate and timely intelligence must serve as its foundation. As they attempt to direct resources against specific enemy C2 nodes or to keep friendly C2 functional in spite of enemy attempts to destroy it, the C2W planning staff depends upon a detailed understanding of such things as the adversary's intentions and capabilities, his strengths and weaknesses, the locations of his forces and their likely actions, the capabilities of his C2 systems, the vulnerabilities of potential C2 targets, and the enemy's counter-C2 capabilities. Each element of C2W has unique intelligence requirements and applications. The general support required by each element is outlined below and summarized in table 6:

OPSEC. Effective OPSEC planning requires detailed information on the capabilities and limitations of the opponent's intelligence gathering system. This includes specific intelligence concerning the means, methods, and facilities the enemy uses to collect, process, and analyze intelligence, as well as any individual or cultural biases that influence his interpretation of the intelligence obtained. OPSEC efforts rely heavily on counterintelligence reporting to ascertain their effectiveness.⁶⁹

PSYOP. PSYOP planners require several types of detailed intelligence information. The PSYOP forces are often oriented to specific regions and have intelligence personnel dedicated to their units to coordinate with the intelligence community for the necessary support. The intelligence efforts focus on the adversary's command, control, communications, computers, and intelligence architecture, including the telephone and facsimile numbers of key command and control nodes as well as data network addresses. They provide basic area studies of foreign cultures and the targeted groups within those cultures, including popular radio and television programs and personalities,

Table 6. Intelligence Support to Command and Control Warfare

PHYSICAL DESTRUCTION	ELECTRONIC WARFARE	OPERATIONS SECURITY	MILITARY DECEPTION	PSYCHOLOGICAL OPERATIONS
Target Identification	Target Location	Friendly Vulnerability Assessments	Identification of Deception Targets	Identification of Enemy Perceptions, Strengths, and Vulnerabilities
Target Location	Electronic Preparation of the Battlefield	Identification of Enemy C2W Threat	Selection of Believable Story	Selection of a Focus of PSYOP Campaign Efforts
Time for Optimal Attack	Frequencies, Critical Nodes, Modulations, and Link Distances	Denial of Friendly Capabilities and Intentions	Identification of Enemy Order of Battle to Include Intelligence Collection Systems	Identification of Enemy Order of Battle to Include Key Commanders and Their Associated C2 Support Systems
Battle Damage Assessment	Time for Optimal Attack	Evaluation of Deception Efforts	Placement of Assets	Placement of Assets
Intelligence Preparation of the Battlefield	Battle Damage Assessment		Analysis and Feedback	Analysis and Feedback
	Joint Restricted Frequency List			

Source: Norman B. Hutcherson, Command & Control Warfare: Putting Another Tool in the Warfighter's Data Base, (Maxwell Air Force Base, AL: Air University Press, 1994), 30.

popular periodicals and cartoons, mechanisms for political control, and important holidays and historical dates. Intelligence efforts determine what target audience is most likely to manifest the behavior required to achieve the PSYOP plan's objectives. They determine the leadership structure (both formal and informal) within the targeted group, as well as the individuals who hold key positions within that structure. They assess what actions are most likely to influence the targeted group and its leaders, and how PSYOP efforts can manipulate those actions to achieve desired objectives. Additionally, intelligence efforts assess the impact that PSYOP operations may have on individuals outside the targeted group--such as multinational partners and populations in neighboring countries.⁷⁰

Military Deception. Intelligence assessments give the deception planner an understanding of the opponent's biases and perceptions on which to base deception operations. The intelligence system provides profiles of key enemy leaders, country studies containing detailed information on cultural, religious, social, and political peculiarities of the country and region, as well as sources of military, economic, or political support. Collection efforts focus on the current force structure and unit locations, as well as the morale, training, capabilities and limitations of those forces. They assess the opponent's current and past PSYOP and propaganda activities and their effectiveness, to include the communications and broadcast systems enemy leaders employ to elicit support from the populace and the country's allies. Deception planners employ assessments of the opponent's decision making processes, patterns, and biases, as well as enemy perceptions of the military situation in the operational area. During the execution of deception operations, intelligence plays the critical role of gauging the enemy's response to the deception, enabling planners to modify, reinforce, or terminate operations as necessary. Their ability to convey a deception story rests with the adversary's intelligence collection system and its ability to convey that story. Planners must also understand the capabilities and limitations of that system to detect the deception story and to manipulate it to their advantage. The intelligence support required for deception operations is similar to that required for both OPSEC and PSYOP. Consequently, support to those three elements requires close coordination to better facilitate the manipulation of the adversary's perception of the battlefield before, during, and after a military operation.⁷¹

Electronic Warfare. EW operations depend heavily on timely, accurate, all-source intelligence. Effective operations rely on both communications intelligence and electronics intelligence products, particularly electronic order of battle and signal data bases.⁷² This information is critical to effective target selection, to the selection and synchronization of assets to engage the targets designated, and to assessments of the effectiveness of the attacks.

Destruction. Intelligence support to physical destruction focuses primarily on the targeting process. It identifies the adversary's C2 systems (including intelligence), the communications

architecture supporting those systems, and the facilities that house them. It assesses the vulnerabilities of the systems and identifies the defensive measures protecting them.⁷³ Once friendly assets strike their targets, intelligence efforts focus on assessing the degree of damage obtained. Planners rely on that information to determine if they have achieved the desired results or if they will strike those targets again.

Although intelligence operations have always been part of warfare, as the world enters the information age they assume even greater importance in the outcome of battles and engagements. Both friendly knowledge of the enemy and situational awareness must be more certain, more timely, and more accurate than the adversary's. Intelligence support to C2W involves more than technological superiority. Although technology is indeed critical in collecting, processing, integrating, correlating, and disseminating information, it is the human process of analyzing and interpreting this information that offers the greatest value to C2W.⁷⁴ Intelligence assessments of the vulnerabilities of C2 targets allow planners to identify and select the appropriate means to conduct C2W operations. Intelligence monitoring activities, prior to and during military operations, provide planners the necessary information to tailor the operations and to gauge the effectiveness of the overall campaign. Intelligence estimates of the enemy's capabilities to exploit friendly vulnerabilities allow planners to determine priorities of enemy targets while increasing protective measures.⁷⁵

Summary

In summary, the synergistic employment of the five elements of C2W provides the operational commander with the capability to deliver a decisive blow against his opponent. It allows him to observe the situation, orient available forces to meet the perceived threat, and act in a quick but effective manner. OPSEC, military deception, and PSYOP combine to effectively disrupt the adversary's perception of friendly intentions. Physical destruction and EW provide an ideal mix, expanding the commander's options to destroy or ignore a target. With intelligence as a bedrock, the commander can achieve the maximum effectiveness of his operations with the integration and employment of C2W.

Endnotes

¹Peter G. Tsouras, Warriors' Words: A Quotation Book (New York, NY: Arms and Armour Press, 1992), 121.

²Daniel E. Magsig, (December 7, 1995). "Information Warfare in the Information Age." [Online]. Available: <http://www.seas.gwu.edu/student/dmagsig/infowar.html>.

³Ibid.

⁴Norman B. Hutcherson, Command & Control Warfare: Putting Another Tool in the Warfighter's Data Base (Maxwell Air Force Base, AL: Air University Press, 1994), xv.

⁵National Defense University, Joint Command and Control Warfare Staff Officer Course: Student Text (Norfolk, VA: Armed Forces Staff College, draft, undated), 3-1.

⁶Ibid., 3-5.

⁷Ibid., 6-2.

⁸Ibid., 6-8.

⁹Ibid., 6-9.

¹⁰Ibid.

¹¹Ibid., 6-9 through 6-10.

¹²Ibid., 6-10.

¹³Ibid.

¹⁴Ibid., 7-2.

¹⁵Ibid.

¹⁶Ibid.

¹⁷Ibid., 7-5 through 7-6.

¹⁸Ibid., 7-5.

¹⁹Ibid.

²⁰Headquarters, Department of the Army, FM 100-6, Information Operations (Washington, DC: U.S. Government Printing Office, working draft, 1995), 3-16.

²¹Hutcherson, 21.

²²Joint Command and Control Warfare Staff Officer Course, 9-1.

²³Hutcherson, 22-23.

²⁴Joint Command and Control Warfare Staff Officer Course, 9-4 through 9-6.

²⁵Hutcherson, 23.

²⁶Chairman, Joint Chiefs of Staff, Joint Pub 3-53, Doctrine for Joint Psychological Operations (Washington, DC: U.S. Government Printing Office, 1993), I-1.

²⁷Hutcherson, 24-25.

²⁸Joint Command and Control Warfare Staff Officer Course, 10-2.

²⁹*Ibid.*

³⁰*Ibid.*, 10-4.

³¹Hutcherson, 25.

³²*Ibid.*

³³*Ibid.*

³⁴Chairman, Joint Chiefs of Staff, Joint Pub 3-58, Joint Doctrine For Military Deception (Washington, DC: U.S. Government Printing Office, 1994), I-1.

³⁵Joint Command and Control Warfare Staff Officer Course, 11-2.

³⁶*Ibid.*, 11-3.

³⁷Headquarters, Department of the Army, FM 90-2, Battlefield Deception (Washington, DC: U.S. Government Printing Office, 1988), 6-2.

³⁸Joint Pub 3-58, Joint Doctrine For Military Deception, I-2.

³⁹*Ibid.*

⁴⁰*Ibid.*

⁴¹*Ibid.*, I-3.

⁴²*Ibid.*

⁴³*Ibid.*

⁴⁴Joint Command and Control Warfare Staff Officer Course, 11-5.

⁴⁵FM 90-2, Battlefield Deception, 1-3 through 1-4.

⁴⁶*Ibid.*, 1-5 through 1-6.

⁴⁷Ibid., 1-6 through 1-7.

⁴⁸Ibid., 1-7.

⁴⁹Ibid., 1-7 through 1-8.

⁵⁰Ibid., 1-9.

⁵¹Ibid., 1-12.

⁵²Ibid.

⁵³Chairman, Joint Chiefs of Staff, Joint Pub 3-0, Doctrine For Joint Operations (Washington, DC: U.S. Government Printing Office, 1993), GL-7.

⁵⁴Chairman, Joint Chiefs of Staff, Memorandum of Policy (MOP) No. 30, Command and Control Warfare (Washington, DC: U.S. Government Printing Office, 1993), A-1.

⁵⁵Joint Command and Control Warfare Staff Officer Course, 13-3.

⁵⁶Ibid., 13-5.

⁵⁷Ibid., 13-6.

⁵⁸Ibid., 13-2.

⁵⁹Hutcherson, 26.

⁶⁰Ibid., 26.

⁶¹Joint Command and Control Warfare Staff Officer Course, 14-2.

⁶²Ibid.

⁶³Ibid., 14-3 through 14-4.

⁶⁴Ibid., 14-4 through 14-5.

⁶⁵Ibid., 14-6.

⁶⁶Ibid., 14-7.

⁶⁷Ibid., 14-10.

⁶⁸Hutcherson, 27.

⁶⁹Chairman, Joint Chiefs of Staff, Joint Pub 3-13.1, Joint Doctrine For Command and Control Warfare (C2W) (Washington, DC: U.S. Government Printing Office, 1996), III-3.

⁷⁰Ibid., III-4.

⁷¹Ibid., III-3 through III-5.

⁷²Ibid., III-6.

⁷³Ibid.

⁷⁴Kerry A. Blout and Lauren D. Kohn, "C2 Warfare in FM 100-6," Military Review LXXV, no. 4 (July-August 1995): 68.

⁷⁵Hutcherson, 31.

CHAPTER 3

APPLICATION OF C2W: THE GULF WAR

...we are going to cut the head off the snake.¹

General Colin Powell, 23 January 1991, speaking of the Iraqi Army

Introduction

This chapter will explore a practical application of the five elements of C2W using the 1990 to 1991 Gulf War, Operations Desert Shield and Desert Storm. The thesis selects this particular war for several reasons:

1. Prior to the Gulf War, the concept of C2W existed as C3CM. It employed OPSEC, deception, EW, and destruction in a primarily defensive role to protect friendly command, control, and communications. Until the end of the cold war, friendly forces did not target enemy C2 in the belief that doing so would generate an escalation of hostilities. The Gulf War was essentially the birth of C2W as an offensive strategy in addition to its defensive applications. Moreover, General H. Norman Schwarzkopf, Commander in Chief of Central Command (CINCCENT) and commander of the Coalition forces during the war, integrated a fifth element--PSYOP--in his attack on Iraqi C2. The Gulf War raised the old concept of C3CM to a new level--that of a supporting strategy rather than solely a collection of defensive measures. It demonstrated how the synergistic application of five diverse elements could bring significant results on the battlefield.

2. Many view the Gulf War as the first Information Age war. C2W optimizes its potential in such an environment. The various elements operate to some degree in any conflict but they achieve their greatest impact in the highly technical environment of the Information Age.

3. Although the Gulf War was unique in many ways, it, nevertheless, demonstrated many capabilities that U.S. military forces will apply in future battles. The lessons it teaches are applicable not just for the next few years but for the next several decades of warfare.

To set the stage for discussion of C2W's role in the war, the opening pages of this chapter will first summarize events leading up to the war, present aspects of the enemy force which facilitated the Coalition's employment of C2W, and outline the Coalition campaign plans that the C2W strategy supported.

Background

In the early morning hours of 2 August 1990, three divisions of the Iraqi Republican Guard Forces Command (RGFC) attacked across the Iraq border into Kuwait. A mechanized infantry division and an armored division conducted the main attack south into Al-Hahra while a second armored division conducted a supporting attack farther west. At the same time, a SOF element conducted a heliborne assault on Kuwait City. The two divisions conducting the main attack continued into Kuwait City where they linked with the SOF forces. By early evening they had secured the capital city and tank formations were continuing south along the coast to occupy Kuwaiti ports. The supporting armored division moved south to occupy blocking positions along main avenues of approach from the Saudi border.²

Hopelessly outmatched, the Kuwaiti military forces could mount only an uncoordinated and futile defense. By 4 August, Iraqi forces had established defensive positions along the Kuwait-Saudi border. Reinforcing divisions began moving south from Iraqi garrisons. These forces would replace the RGFC units already in Kuwait, freeing these elite forces for possible subsequent attacks into Saudi Arabia. By 8 August, more than 200,000 soldiers supported by an excess of 2,000 tanks were consolidating their gains in Kuwait. Saddam Hussein, the military and political ruler of Iraq, announced the annexation of the country, declaring Kuwait the "19th Province--an eternal part of Iraq."³

World condemnation was swift. Galvanized largely by the United States, an international Coalition formed to force Saddam from Kuwait. Nearly fifty countries contributed resources of some form to the effort. Thirty-eight of those countries deployed air, sea, or ground forces. They contributed assets totaling more than 200,000 troops, 60 warships, 750 aircraft, and 1,200 tanks.⁴ They sought to compel Iraq to relinquish its control of Kuwait first by diplomatic means but then with force if necessary.

Saddam refused to alter his resolve to hold Kuwait. By January 1991, he had an estimated force of 500,000 arrayed in defensive positions in Kuwait. At least two defensive belts extended along southern Kuwait and along the Kuwaiti coast including formidable triangular fortifications along the Saudi border. These defensive belts included minefields and oil-filled fire trenches covered by interlocking fields of fire from tanks, artillery, and machine gun positions. Coastal positions hosted numerous naval and land mines. RGFC forces formed strong, mobile, heavily armored counterattack forces ready to blunt any Coalition penetration of defensive positions.⁵

During their months of occupation, Iraqi forces constructed an impressive system of roads, buried communications lines, and supply depots. They also buried command posts, often under as much as twenty-five feet of desert sand. Such an infrastructure did much to multiply the combat power of the deployed forces. It enabled reinforcements and supplies to move over multiple routes to any point on the battlefield. Buried telephone lines and fiber optic cables dedicated to command and control offered poor targets for attack.⁶

Despite Iraq's numerical strength and extensive military infrastructure, Coalition intelligence discerned a number of significant weaknesses, several of them with direct import to a C2W strategy: (1) A rigid, top-down C2 system controlled the Iraqi military. It discouraged and even punished initiative by its unit commanders. (2) The desert environment made military forces and facilities particularly vulnerable to air attacks. (3) The Iraqi military demonstrated a generally defensive approach to battle; they had only a limited ability to conduct deep operations. (4) The military forces exhibited uneven qualities and capabilities. The force centered on the elite RGFC units which, though

best trained, equipped, and capable, had limited numbers. The larger Regular Army, for the most part, received a lower priority for training and receipt of new equipment and demonstrated varying degrees of combat readiness. (5) The Iraqi leadership had a faulty understanding of the Coalition forces' operational capabilities. (6) Iraq could not effectively interfere with U.S. space-based assets. (7) Iraq had only a limited air offensive capability. And (8) Iraq had no effective foreign intelligence.⁷

In addition to these weaknesses, Coalition planners identified one of the major Iraqi centers of gravity⁸ as the command, control, and leadership of the Saddam Hussein regime. If it lost its ability to direct the military forces or to control its civilian population, Iraq might be forced to comply with Coalition demands.⁹

The nature and structure of the Iraqi C2 system, coupled with the weaknesses identified in the military forces offered unique opportunities for exploitation in a C2W strategy. Coalition planners were quick to seize these opportunities. The mission statement which transitioned Central Command (CENTCOM) from defensive to offensive operations established as its first objective the "neutralization [of the] Iraqi National Command Authority."¹⁰ CENTCOM's subsequent Operations Order (90-001, dated 17 January 1991) stated as its first theater military objective an "attack [on the] Iraqi political-military leadership and C2."¹¹ This focus from General Schwarzkopf, as the CINCCENT, the highest level of command in the theater, ensured that commanders at all levels emphasized C2W planning and execution. The campaign plans of the component forces amply demonstrate this.

Overview of the Air Campaign Plan

The air campaign provided the Coalition with an offensive option in the early fall of 1990 before adequate ground forces could arrive in the theater. The strategic plan focused on Saddam Hussein's vital centers of gravity. It sought to paralyze the Iraqi leadership's ability to command and control its forces, to destroy known Iraqi weapons of mass destruction, to render Iraqi forces in the Kuwait theater combat ineffective, to prepare the battlefield for ground force operations, and to minimize the loss of life for Coalition forces. Planners designed the air campaign into three phases

whose success depended on overwhelming the Iraqi military command structure and air defenses, gaining accurate intelligence, exploiting technological advantages, and, ultimately, on the ability of the combat crews. Once the air attacks could bring the ratios of combat power to an acceptable level, and if Iraq failed to comply with U.N. demands, multinational air and ground forces would launch a coordinated combined arms attack to eject Iraqi forces from Kuwait. With enough air forces on hand in January, Coalition leaders elected to execute the three phases of the air campaign almost simultaneously, thus applying overwhelming pressure from the opening minutes of the war.¹²

Overview of the Ground Campaign Plan

The ground campaign plan centered on a main attack in the form of a "left hook" by armor-heavy forces against Iraq's right flank, sweeping in from the west to avoid most fixed defenses and to attack one of Saddam Hussein's centers of gravity, the Republican Guard armored and mechanized divisions. The success of the plan hinged on overwhelming combat power; rapid maneuver; deception; a sound, combined arms approach; a well-trained, highly motivated body of troops; and a skilled team of combat leaders in the field. The main attack relied on an elaborate deception operation, including an amphibious feint, and on supporting attacks along the Kuwaiti-Saudi border to fix Iraqi forces in Kuwait and to liberate Kuwait City.¹³

Overview of Maritime Campaign Plan

In addition to supporting the air campaign, the maritime campaign plan had the primary objective of developing and maintaining the capability to launch an amphibious invasion along the Kuwaiti coast. Although the invasion did not occur, the Naval Component of Central Command (NAVCENT), had to present a credible threat in order to convince Iraq to commit a substantial part of its military forces to defending against that threat. To present this amphibious threat, maritime forces first had to perform extensive antisurface warfare (ASUW), mine countermeasures (MCM), and naval gunfire support (NGFS) operations. They were also responsible for defending the coastlines of Saudi Arabia, the United Arab Emirates (UAE), Qatar, Bahrain, Oman, and the adjoining

maritime areas. During the eight years of the Iran-Iraq War, Iraq demonstrated capabilities that could threaten Coalition ports, such as Ad-Dammam and Al-Jubayl, as well as Coalition naval forces operating in the Gulf.¹⁴

The Command and Control Warfare Strategy

Deception

Throughout the planning process, CINCCENT insisted on a comprehensive plan to deceive Saddam Hussein regarding Coalition intentions and to conceal the Coalition scheme of maneuver. The deception plan centered the attention of the Iraqi forces to the south of Kuwait, convincing them that the Coalition's main attack would be directly into Kuwait supported by an amphibious assault on the coast. The plan diverted Iraqi forces from the Coalition's main effort in the west and, instead, ensured that Iraqi divisions remained fixed in eastern Kuwait and along the Kuwaiti coast.¹⁵

All components played vital roles in the deception story. The Air Force Component of Central Command (CENTAF) established a highly visible pattern of air activity round-the-clock. Its placement of air refueling tracks and training areas emphasized preparations to support a frontal assault against entrenched Iraqi defenses and reinforced Iraq's beliefs about Coalition intentions.¹⁶

CENTAF conditioned the Iraqis to the presence of large numbers of Airborne Warning and Control System (AWACS)¹⁷ aircraft and fighter combat air patrols (CAP) on the borders with Saudi Arabia and the Persian Gulf. These aircraft flew defensive missions in the same orbits and numbers they would fly in the air offensive. A series of surges began to create a pattern of increased activity one night a week.¹⁸

The final preparations for transition to offensive operations placed many aircraft on ground alert. CINCCENT explained it as a precaution against a preemptive Iraqi attack prior to the 15 January U.N. deadline. The true reason was to allow mission planning, crew rest, and aircraft reconfigurations without revealing the Coalition's actual intentions. Ground alert weapons loads matched the loads listed in the air tasking order (ATO) for the attack. However, F-15 aircraft few daily operational CAP missions within range of Iraqi radars and could not stand down without leaving

Saudi airspace unprotected and generating Iraqi suspicions. To maintain the perception of routine Coalition operations yet also allow F-15 units to make final preparations, F-16s not involved in the first attack filled the defensive gaps.¹⁹ The air strike force was able to marshall out of range of Iraqi radar coverage while F-16 CAPs convinced the Iraqis that routine operations continued. Strike force packages thus entered Iraqi airspace with minimal warning and maximum surprise.

In support of the theater deception plan, amphibious warfare planners developed plans ranging from large-scale amphibious assaults into Kuwait to raids and feints on islands and coastal areas. Additionally, the amphibious task force (ATF) provided a critical seaborne threat to the flank of Iraqi forces--forces in a position to attack Saudi Arabia along the main coastal road from Ras Al-Khafji to Ad-Dammam. The ATF conducted several amphibious exercises along the eastern Saudi Arabian coast and in Oman. The highly publicized operations ensured the Iraqi command understood the Coalition's amphibious capabilities. An amphibious raid on the Umm Al-Maradim Island off the southern Kuwaiti coast further magnified Iraqi fears of a coastal invasion and reinforced the theater deception plan.²⁰

The amphibious exercises, feints, and demonstrations conducted by the ATF focused the Iraqi command's attention on the coast of Kuwait. In large measure, this preoccupation with Kuwait, and particularly against an amphibious assault, facilitated the ground offensive's left hook maneuver. The amphibious invasion was not an idle threat; otherwise, its support to the deception story would have been negligible. Had the situation required, the ATF could have conducted a successful assault--although possibly with substantial casualties. Although events did not force a major amphibious operation, the ATF, nevertheless, played a crucial role in the overall success of Operation Desert Storm. Iraq's refusal to evacuate coastal defenses even when ground forces were encircling its rear, testified to the effectiveness of the amphibious effort.²¹

Ground force units conducted reconnaissance and counter reconnaissance operations with Iraqi forces to deny them information about actual Coalition intentions. For thirty days prior to the ground offensive, the 1st Cavalry Division conducted aggressive feints, demonstrations, and artillery

raids in the direction of Iraqi defenses nearest the Wadi Al-Batin. These actions further reinforced the Iraqi belief that the Coalition would launch its main attack directly north into Western Kuwait. They held five infantry divisions and an armored division in place in Kuwait, well away from the actual VII Corps zone of attack.²²

As maneuver forces began the shift west after the launch of the air campaign, Task Force Troy, consisting of infantry, armor, reconnaissance, engineers, Seabees, and Army PSYOP elements created the impression of a much larger force, engaging enemy elements in the Al-Wafrah area, conducting deceptive communications, and building dummy positions.²³

Throughout the air campaign, ground forces south of Kuwait aggressively conducted raids, patrols, feints, and long-range reconnaissance. In addition to gaining additional information on the extent and locations of Iraqi obstacles and defensive positions, they prevented the Iraqis from discovering Coalition force dispositions to their south and continued to reinforce the threat of attack directly north into Kuwait.²⁴

As the ground offensive began, the 1st Cavalry Division feinted toward Wadi Al-Batin. Task Force Troy demonstrated along the southern Kuwaiti border to conceal the true location of the Marine attack. These efforts, coupled with a supporting attack by two Marine divisions into the “shoulder” of Kuwait, an obvious avenue of approach, and several demonstrations by the 4th Marine Expeditionary Brigade (MEB) off Ash Shuaybah, Bubiyan Island and Faylakah Island, served to fix the Iraqi forces in place and preclude a shift to the west to meet the main attack or to reinforce Iraqi forces to the west. When Coalition forces swept in from the west, they found their Iraqi foes oriented to the east and south, allowing them to conduct devastating attacks against their flanks and rear.²⁵

The deception efforts were not one-sided. Iraqi military forces and intelligence services conducted a somewhat sophisticated, albeit limited, military deception program directed against Coalition commanders, intelligence services, policy makers, and foreign populations. Relying primarily on Soviet methods and training, Iraqi deception efforts sought to reduce the effectiveness of Coalition air strikes, enhance the survivability of Iraqi forces, destabilize the Coalition, and

increase uncertainty about Baghdad's future intentions. The Iraqi effort failed to mislead Coalition intelligence activities regarding their overall military capabilities and intentions; however, they certainly complicated the Coalition effort.²⁶

The Iraqis employed a number of active measures to present a false picture to the Coalition. These included both simulations, such as decoys, and disinformation programs. They painted false bomb craters on undamaged runways and constructed false positions, including some dummy SAM and Silkworm missile sites. They employed decoy missile attack boats, artillery pieces, and tanks. Their decoy positions succeeded in drawing fire and enhancing the survivability of other operational equipment. Night capable smart munitions negated this ruse when no heat source was present. Soon, however, the Iraqis began to place burning tires in or near the equipment to simulate a heat signature. As Coalition aircraft engaged from even shorter ranges, this ploy lost its effectiveness; however, for a time, it succeeded in drawing fire from more lucrative targets. Decoy Scud missile launcher sites, some employing heat producers to simulate active generators, complicated Coalition efforts to eradicate the Iraqi ballistic missile threat.²⁷

Some Iraqi industrial complexes served dual purposes in an effort to conceal their military value. In one example, Iraq unsuccessfully tried to hide a biological agent production facility in a factory producing infant formula. Although that deception effort was unsuccessful, Iraq successfully concealed other unconventional weapon facilities. The Iraqi disinformation program sought world condemnation of the U.S. for destruction of the infant formula plant until U.S. statements made it clear that the facility had a biological warfare role.²⁸

U.S. intelligence unmasked several Iraqi deception efforts, such as the simulated destruction of a mosque. Similar damage in downtown Baghdad, blamed by Iraq on U.S. planes, was, in fact, caused by Iraqi antiaircraft artillery (AAA) fire and SAMs fired without guidance. Nevertheless, concerns about negative publicity resulted in a decision to curtail bombing in downtown Baghdad after February. Iraq planted disinformation stories in the Coalition press, such as the U.S. military consorting with Egyptian concubines, shooting Moroccan soldiers, or defiling Islamic holy sites.

Although this disinformation campaign incited some Arab opposition against the Coalition and the U.S., it did not cripple the execution of Operation Desert Storm. Similarly, Iraq failed in its pre-hostilities efforts to paint Kuwait as unworthy of international support and thereby block the formation of the Coalition altogether. The Coalition scorned Iraqi predictions of “the mother of all battles,” “10,000 U.S. casualties in a single day,” or the “destruction of the Arab nation.”²⁹

Although the U.S. was generally aware of Iraqi deception and disinformation measures, they, nevertheless, enjoyed some degree of success by causing the Coalition to direct munitions against decoy targets and by making the campaign against the military infrastructure more difficult and more susceptible to propaganda exploitation.³⁰

Operations Security

OPSEC’s most significant role in the Gulf War was in support of the Coalition’s deception operation. The two went hand-in-hand. From the initial deployment of forces until the initiation of the air war, the personal attention of the CINCCENT ensured that all participants employed extensive measures to safeguard the deception story.

When Coalition forces began to build up south of Kuwait, Iraq began to feed additional divisions into Kuwait to strengthen their defenses. As the Coalition buildup expanded to the west, Iraqi forces, likewise, shifted to positions opposite those forces. Such actions were sure to compromise the ground forces’ plan of attack; therefore, General Schwarzkopf halted an early buildup of combat forces in the west. Instead, those forces deployed to base camps in eastern Saudi Arabia and moved to attack positions only under cover of the air campaign. Likewise, the general vetoed a proposal to begin a near-term buildup of supplies at King Khalid Military City in preparation for the offensive. Although a prudent measure to ensure logistical support, it would have given a clear indication of Coalition attack plans.³¹

In several cases the OPSEC measures enforced generated consternation among subordinate commanders; in some cases they levied additional workloads on subordinate staffs. For example, OPSEC prevented the ground commanders assigned to the western attack sectors from conducting

intelligence collection operations to the depth of their respective areas of interest.³² Instead, they initially had to rely on the echelons above corps intelligence systems and organizations for detailed intelligence support. Likewise, by CINCCENT direction, air operations did not target Iraqi forces to the west until just prior to the ground war. Although this enhanced the deception story, it concerned those western-oriented ground force commanders who naturally sought air power to degrade the enemy units immediately in their line of advance.³³

With the air campaign, Coalition ground forces launched extensive counter reconnaissance efforts which effectively prevented Iraqi reconnaissance from discerning the true direction of the Coalition attack. With Iraq effectively blinded, more than 270,000 troops made the move west--some units shifting more than 260 miles. This movement, which continued twenty-four hours a day for more than three weeks, constituted one of the largest and longest movements of combat forces in history. Whole divisions and extensive support structures moved hundreds of miles--undetected by the Iraqis.³⁴

Psychological Operations

Psychological operations played a key role in the Gulf War. The Saudis were particularly clever in directing leaflets and radio broadcasts at "fellow Arab" Iraqi soldiers. In some ways Saddam Hussein made the task easy. He was not particularly popular to begin with and the Saudis could easily blunt his religious appeals.³⁵

The Coalition PSYOP campaign focused on six primary objectives: (1) to gain acceptance and support for U.S. operations; (2) to encourage Iraqi disaffection, alienation, defection, and loss of confidence; (3) to create doubt in Iraqi leadership; (4) to encourage noncooperation and resistance; (5) to strengthen confidence and determination of friendly states to resist aggression; and (6) to improve the deterrent value of U.S. forces. PSYOP forces aggressively pursued these objectives. They employed leaflets and radio broadcasts to undermine unit morale, to provide instructions on how to surrender, to instill confidence that the Coalition would treat prisoners humanely, and to provide advanced warning of impending air attacks, thus encouraging desertion. After the cease fire, an Iraqi

division commander stated that next to the Coalition bombing operations, PSYOP was the greatest threat to his troops' morale.³⁶

The PSYOP effort focused on breaking the Iraqi will to resist and on increasing the fears of Iraqi soldiers. At the same time, it highlighted that the Coalition did not oppose the Iraqi people--only Iraq's national policy.³⁷ In one especially effective tactic, leaflet drops exploited the success of the B-52 carpet bombings. Even when the iron rain from the B-52s did not strike their targets, the effect on the soldiers' morale was devastating. Forces at distances in excess of 100 kilometers could hear the attacks. At times, they could feel the ground tremors as much as 200 kilometers away from the target area. After such attacks, PSYOP specialists dropped leaflets containing a picture of a B-52 along with information in Arabic which specified the date and time the next wave of B-52s would "visit" the Iraqi troops in the target zone. And just as prophesied, the B-52s arrived.³⁸ One Iraqi officer attributed his surrender to the B-52 strikes. "But your position was never attacked by B-52s," his interrogator commented. "That is true," the Iraqi officer stated, "but I saw one that had been attacked." After one bombing of an Iraqi minefield, B-52s dropped leaflets on Iraqi troops who had witnessed the explosion, warning they would be next. Not knowing the bomb had struck a minefield, mass defections resulted, including virtually the entire staff of one Iraqi battalion.³⁹ Suddenly, the PSYOP leaflets had a newfound credibility and encouraged many Iraqis to surrender. Further, the leaflets promised good treatment for prisoners. They emphasized that the Coalition's intent was not to destroy Iraqi troops but to force Iraqi leaders to leave Kuwait. They instructed Iraqi soldiers to stay away from their equipment because they would destroy it but spare the soldiers. This instilled a perception of humanity, for suddenly the Iraqi soldier was not confronting heartless infidels.⁴⁰

Twenty-nine million leaflets consisting of thirty-three different messages fell in the Kuwait theater of operations. The campaign followed a building block approach with the first leaflet themes being ones of peace and brotherhood. As the situation evolved, the intensity of the messages increased and transitioned to an emphasis on the U.N. imposed 15 January deadline. Once that

deadline passed and Operation Desert Storm began, PSYOP themes shifted to encourage desertion, to emphasize the abandonment of equipment, and to exploit the B-52 bombing raids.⁴¹

Broadcast operations supplemented the leaflet campaign and enabled Coalition forces to reach Iraqi soldiers and civilians with more sophisticated messages. The Air National Guard Special Operations flew EC-130 Volant Solo aircraft specially configured with radio transmitters to support PSYOP. Three ground stations and a joint U.S. and Saudi television station augmented broadcast efforts.⁴² The "Voice of the Gulf," the Coalition's radio station, broadcast from 19 January until the end of the war and, according to some claims, served as the most reliable source of war news available to the Iraqi soldier throughout Desert Storm.⁴³

The PSYOP campaign also made effective use of loudspeaker teams. Each tactical maneuver brigade moved with attached loudspeaker PSYOP teams. The teams accompanied the units into Iraq and Kuwait, broadcasting tapes of prepared surrender messages. Cross cultural teams developed the Arabic messages along themes similar to the leaflets. They encouraged Iraqi soldiers to surrender, warned of impending bombing attacks, and promised fair, humane treatment to those who surrendered. Many enemy prisoners of war (EPW) stated they heard the loudspeaker broadcasts in their area and surrendered because they feared more bombing.⁴⁴

Overall, psychological operations played a key role in the destruction of enemy morale and played a major part in the large-scale surrender and desertion of Iraqi soldiers. Leaflets and broadcasts not only had great impact on Iraqi morale, they also provided information which gave the Iraqi soldier detailed instructions on how to surrender, instilled confidence that their Coalition captors would treat them fairly and humanely, and provided advance warning of impending attacks, allowing them to save their lives. The reach of PSYOP was clearly evident from the number of Iraqis who surrendered with PSYOP leaflets clutched in their hands and from the numerous EPWs who, when debriefed, repeatedly cited the PSYOP efforts as a factor in convincing them to surrender.⁴⁵

Electronic Warfare

Compared to the deception and PSYOP activities, the Coalition's employment of electronic warfare lacked drama and media attention. It was, nevertheless, vital to the success of the entire war effort. The war demonstrated lessons in all the elements of EW--electronic support, electronic attack, and electronic protect--with a scope and sophistication that far exceeded anything previously witnessed. The EW investment made in the 1980s defense buildup envisioned a Soviet-NATO conflict in central Europe. Continuously refined in numerous U.S. exercises against an expected formidable Soviet threat, Coalition EW triumphed against the much weaker Iraqi capabilities. In the opening minutes of the war, the Coalition's EW completely disrupted Iraq's command, control, communications, and intelligence (C3I) system. It severed the command links from Baghdad to the field forces, contributing to the spectacular collapse of the Iraqi military forces as soon as the ground offensive began. In the air war, EW magnified the impact of Coalition air power, which quickly defeated Iraqi air defenses and minimized losses of Coalition aircraft. In the words of one U.S. pilot, "If it had not been for [EW] . . . 50% of our aircraft would not have returned."⁴⁶ EW also enabled the Coalition to look deep into the Iraqi operational and strategic depths, while denying them the same advantage, and it contributed substantially to the stunning success of the deception story that accompanied the ground offensive.

Iraq employed an extensive air defense umbrella consisting of some 17,000 SAMs, nearly 10,000 AAA pieces, and a wide variety of sophisticated communications links. In spite of this, Coalition aircraft suffered minimal losses. A major factor in this imbalance was the fact that the Iraqis had made a minimal investment in EW technology in the decade preceding the Gulf War. They never faced a technically sophisticated air threat from Iran nor did they fear the capabilities of any of their Arab neighbors. Thus, they took only limited steps to modernize their air defense systems. Although Iraq supported what some have termed the world's fourth largest army, it did so with a gross national product (GNP) about equal to Portugal's. The military sacrificed much to achieve and maintain its force structure. With such a massive military based on a Third World economy, there

were far too few technical personnel to support the military and its associated industries. In compensation, Iraq relied heavily on foreign advisors and technicians, especially Soviet advisors. When they withdrew with the threat of impending war, the loss weakened Iraq's already limited EW capabilities.⁴⁷

Electronic Support. The Coalition continuously conducted an extensive ES campaign, collecting and analyzing electronic emissions to yield a comprehensive intelligence picture. Its specialized ES aircraft inventory included three U.S. Air Force RC-135s, including the RC-135V/W Rivet Joint models. U-2Rs collected communications intelligence (COMINT), in some cases relaying intercept data in real time through a wideband satellite link. British Royal Air Force Nimrod R.2s deployed and the French provided a DC-8 Sarigue, an EC-160 Gabriel, plus two modified SA330 Puma helicopters. EW combat aircraft, such as the U.S. Navy's EA-6B and Air Force's F-4G, EF-111A, and possibly RF-4Cs worked to refine the electronic order of battle before the war began.⁴⁸

Special Forces electronic warfare teams used both ground and air assets to conduct signal monitoring and radio direction finding operations against Iraq during the early stages of Desert Shield. They established joint and combined electronic listening posts to detect and monitor Iraqi signals. Their reports played a significant role in pinpointing the locations of the Iraqi military command infrastructure and artillery observers for targeting during the initial phase of the air war.⁴⁹

The U.S. Navy's EP-3E and EA-3B forces also reportedly had aircraft in the Gulf and the Air Force's TR-1As added to the COMINT collection and radar surveillance efforts. U.S. Army ES aircraft, both fixed-wing (including RC-12s and RV-1D Quick Looks) and helicopters (including EH-60A Quick Fix IIBs) supplemented these assets, providing intelligence vital to the rapid outflanking movements of the ground campaign. At sea, eight U.S. submarines employed ES to conduct surveillance and reconnaissance operations, and also provided indications and warning for carrier battle groups. In addition to the ES capabilities on its surface combatants and submarines, the Navy employed "bolt-on" electronics intelligence (ELINT) and COMINT systems. The French electronic research ship *Berry*, reportedly configured for ES missions, also operated against Iraq.⁵⁰

A variety of space-based systems further enhanced the Coalition's electronic capabilities. The Gulf War saw an unprecedented use of satellites for communications, navigation, and intelligence. Geostationary U.S. ELINT satellites, including two Magnum and a Vortex, maintained orbits over the western Indian Ocean to provide information on Iraq. KH-12 satellites reportedly provided both imagery and ELINT information. The ELINT satellites were able to provide information to field commanders with unprecedented timeliness. Improved connectivity between U.S.-based processing facilities and theater headquarters made this possible, using Constant Source and Tactical Exploitation of National Capabilities (TENCAP) programs that considerably expedited the flow of intelligence. Ground-based strategic ELINT sites capable of supporting the Coalition effort included U.S. stations in Turkey, Saudi Arabia, the United Arab Emirates, and Oman; British stations in Cyprus and Oman; and French facilities in Djibouti.⁵¹

Combat Electronic Warfare and Intelligence (CEWI) battalions, organic to U.S. heavy divisions, also greatly enhanced the Coalition's ES capabilities. With their broad range of EW capabilities, these units worked closely with corps-level military intelligence brigades to provide a constant integration of ES with EA, hard-kill weapons, and intelligence gathering. Iraqi communications became one of their first victims. When SOF forces interdicted the Iraqis' extensive landline communications networks, to include their fiber-optic systems, the Iraqis were forced to turn to nonsecure radio links, easily intercepted and exploited by COMINT forces or destroyed by hard-kill weapons.⁵²

Most tactical aircraft as well as many helicopters, carried the radar homing and warning (RHAW) receivers, the most common ES systems. The ES problem encountered in several previous conflicts--adapting systems and threat libraries of electronic signatures originally designed against Soviet threats to include Western designed threats--did not recur. During the 1979 Iran hostage crisis and the Falklands War, U.S. and British forces were initially unprepared to counter threats from Western-designed gear, but in 1991, equipment and tactics existed to counter systems, such as captured IHAWK SAMs and Exocet air-to-surface missiles (ASM) and surface-to-surface missiles

(SSM). This was due in large measure to the five months between the force deployments and the beginning of the war.⁵³

The Coalition air campaign could not totally destroy Iraqi ES capabilities which included both Soviet- and Western-designed systems. Although the attacks rendered the Iraqi high command blind, deaf, and unable to move forces in response to information, the residual Iraqi ES capability still presented some degree of danger to the secrecy of the shift of Coalition forces westward. To counter it, Coalition forces redeployed in radio silence while bogus radio transmissions in the original assembly areas provided a flow of radio traffic that convinced Iraqi ears that the units had not moved.⁵⁴

Iraq effectively employed COMINT information to move its mobile Scud missile systems away from incoming air strikes, to turn off radar from defense suppression strikes, and to ambush low-flying attack aircraft. Iraqi ES detected Coalition standoff jamming before strike aircraft came over their targets, alerting AAA to open fire. The Coalition countered by discontinuing jamming support for some F-117 strikes so that the aircraft remained largely undetected; on other occasions, jamming efforts sought to intentionally trigger fruitless Iraqi AAA barrage firings. Iraq monitored the rescues of downed Coalition air crews but could not exploit this information to interfere with operations. They did, however, use ES equipment against Kuwaiti resistance elements.⁵⁵

Electronic Attack. EA, the most dynamic element of electronic warfare, attacks enemy electronic emitters using both active measures that involve radiating electromagnetic energy and passive measures that do not. The Gulf War saw both widely employed.⁵⁶

Coalition forces engaged in heavy jamming. With the possible exception of some non-Saudi Arab forces, every fixed-wing tactical aircraft that crossed the front lines carried an internal jammer or a podded one. This allowed them to operate largely at medium altitudes out of reach of visually-directed AAA and heat-seeking SAMs, thereby reducing aircraft losses. In similar fashion, many helicopters also carried onboard self-protection EA gear. The U.S. Air Force's EF-111A along with the Navy-Marine Corps' EA-6B constituted the Coalition's most formidable EA capability. Both

carried the powerful ALQ-99 jamming system which was highly effective against Iraqi low-frequency, early warning radars and higher frequency target-track and acquisition radars, providing an effective umbrella for strikes. These platforms flew continuous missions during the war, escorting air strikes and providing jamming support that enabled tactical aircraft to penetrate to their targets. Initially, the Navy and Marine Corps did not launch strikes without EA-6B support to prevent Iraqi SAM systems from acquiring the strike aircraft. Attack forces could reduce their jamming efforts as the war evolved because of the apparent success of high-speed anti-radiation missiles (HARM) and other hard-kill weapons in degrading Iraqi air defense capabilities.⁵⁷ Eight EC-130H Compass Call aircraft performed the air communications jamming mission. Their systems also had a “spoofing” capability enabling them to invade enemy communications nets. These aircraft, coupled with surface-based jammers, such as those organic to CEWI battalions, and accurate air strikes severed the control links from Saddam’s centralized national command authority to his troops. At the tactical level, air defense radars could not receive target data during jamming operations. They were forced to light up and search for targets, becoming vulnerable to the devastating attacks of HARMs. This communications severance was very complete. The captured diary of one Iraqi air defense battery commander revealed that he did not hear from his superiors for the last three weeks of the war!⁵⁸

The Iraqis focused their active jamming mainly on ground-based systems. They employed a range of Soviet- and older French-designed ground-based jammers that had little effect against the more modern Coalition systems. Their use of the Paint Can, van-mounted jammers in attempts to jam the E-3A AWACS prior to the onset of hostilities proved futile as Coalition forces easily countered them. Likewise, both the AWACS and the tactical fighters overcame Iraqi jamming during the war itself.⁵⁹

To defeat C3I and air defense, Coalition forces judiciously employed EA, ES, and hard-kill weapons so that each complemented the effects of the other. Frequently, hard-kill weapons are the warfighter’s first choice; in the words of one Israeli general, “the most effective EA is a bomb on a radar station.” However, bombs, “smart” missiles, and the like do not exist in unlimited quantities,

and it is not practical to destroy every target. EW measures frequently offer a safer and more cost effective means of negating a target. The Coalition employed a variety of hard-kill systems, including the F-4G "Wild Weasels," F-117s, F-16s, EA-6Bs, and F/A-18s. During the first ten days of the air campaign, U.S. forces alone flew more than 1,000 sorties against Iraq, firing around 600 HARMs. Attacks on the key nodes of the Iraqi C3 system in the first hours of the war were so destructive that Iraq never recovered. In the opening minutes of the air campaign, U.S. Army AH-64 Apache helicopters destroyed two Iraqi radars, opening strike corridors for fixed-wing aircraft flying in to repeat the process throughout Iraq. Numerous similar aircraft strikes followed, led by U.S. Navy Tomahawk cruise missiles and Air Force F-117s and F-4Gs.⁶⁰

The Coalition employed passive countermeasures far beyond the near-universal use of chaff seen in earlier conflicts. U.S. Navy and Marine Corps tactical aircraft made extensive use of tactical air-launched decoys (TALD) to saturate, confuse, and deceive the Iraqi air defense system. The forces also made extensive efforts to reduce the radar cross-section of a wide range of ships and aircraft.⁶¹

The F-117 Stealth fighter does not use passive countermeasures. Rather, it is a passive countermeasure and an excellent example of how EA has progressed from a peripheral "add-on" to an integral part of a system. Although the F-117s represented only 2.5 percent of the Coalition's tactical air power, they struck 31 percent of the targets hit in the first day of the war and had responsibility for more than 40 percent of all targets. While they were not invulnerable to detection, they demonstrated the increased importance of passive countermeasures in the face of modern weapons.⁶²

Electronic Protection. The most basic EP tactic is emission control (EMCON), minimal radiation of electromagnetic energy vulnerable to ES or EA. Radio or radar silence represents its most extreme application. The Coalition frequently encountered difficulties in maintaining effective electronic discipline. While U.S., British, French, and NATO forces have spent years trying to reverse lax communications security practices commonplace in the past (with varying degrees of

success), some Coalition forces, particularly the Saudis, had no such discipline.⁶³ Against a more technologically advanced opponent, such a vulnerability could have been more lethal.

Iraq, on the other hand, used EMCON extensively--albeit more from fear of Coalition attacks than from good discipline. Nevertheless, the Iraqis minimized their use of radios and air defense radars during Desert Shield, thereby reducing the ELINT available to Coalition intelligence efforts. With the launch of the air war, Iraq turned to their air defense radars only to have them quickly silenced by Coalition attacks. On January 23, the Iraqis activated ninety-five percent fewer radars than they operated on the 17th. Frank Kendall, U.S. Undersecretary of Defense for tactical warfare programs, summed up the situation with the observation, "the willingness to turn on [their] radars and fight doesn't seem to be there."⁶⁴

The Iraqis were also quite good at controlling radar emissions from their missile sites until the last moment. Their procedures were similar to other Arab and Vietnamese users of Soviet-made air defense systems in that they switched to the less accurate but safer optical guidance mode for their SAMs and AAA. The low number of Coalition aircraft lost to SAMs attests to the ineffectiveness of this method.⁶⁵

EP also came into play in the secure, reliable communications employed by Coalition forces. Systems such as the U.S. Army's single-channel ground and airborne radio system (SINCGARS), the Air Force's Have Quick radio, and the Navy's Link 11 data link had integral EP capabilities. Iraq had first and second generation secure radios with EP capability but failed to use them effectively.⁶⁶

Destruction

The Coalition's use of destruction to affect Iraqi C2 achieved its most spectacular results in the early hours of the air war. Critics argue that Desert Storm was an anomaly, that the U.S. will never again have such an advantage over an adversary. However, all modern industrial and military powers share certain universal vulnerabilities. The technological advances that made them powerful also constitute some of their greatest weaknesses. Examples include computer dependent C3 systems, networked air defense systems and airfields, and easily located sources of energy. With the

destruction of their key nodes, such systems suffer cascading and potentially catastrophic failure.⁶⁷ Perhaps the Coalition's effective targeting of these systems helped generate that overwhelming advantage in what otherwise would have been a very different war.

Coalition air campaign planners established as one of their primary objectives⁶⁸ the task of isolating and incapacitating the Iraqi regime. Specifically, they would aggressively target leadership command facilities, electrical production facilities powering military and military-related industrial systems, and telecommunications and C3 systems. Before they could adequately pursue these targets, however, they had to reduce the effectiveness of Iraqi air forces and ground-based air defenses. Therefore a second objective of the air campaign sought to gain and maintain air supremacy to permit unhindered air operations. Its goals for destruction included Iraq's strategic integrated air defense system (IADS), including radar sites, SAMs, and IADS control centers; air forces and airfields.⁶⁹

Leadership Command Facilities. The Coalition intended to fragment and disrupt the Iraqi political and military leadership by attacking the C2 of its military forces, internal security elements, and key nodes within the government. In Iraq's rigid, authoritarian society, where the highly centralized decision-making power rested only in the hands of Saddam Hussein and a few others, destruction of C2 had a particularly crippling effect on forces in the field. Bombing attacks on several leadership facilities, places from which Saddam controlled operations, forced him and other key leaders to avoid the facilities designed and best suited for C3. It drove them to hide and to make frequent moves, severely reducing their ability to communicate with subordinate leaders and military forces, with the civilian population, and with the outside world. They found it impossible to control or even keep pace with events. It also caused them to use less secure radio communications rather than their built-in land line and fiber optic systems, thereby offering valuable intelligence to Coalition collectors.⁷⁰

Coalition forces employed laser-guided artillery rounds, Hellfire missiles, and the Army Tactical Missile System (ATACMS) to strike Iraqi ground force headquarters, conduct counter-battery fire, and suppress air defenses. Indirect fire units focused on destroying the command, control,

communications, intelligence, and fire support capabilities of the first-echelon Iraqi divisions. Overall, Coalition efforts so severely degraded Iraqi C2, that Saddam Hussein was unable to direct his fielded forces and, in numerous occasions, forward corps, division, and brigade commanders completely lost touch with their subordinate commands. The destruction levied on the Iraqi forces, coupled with the Coalition's skillful PSYOP campaign, sapped Iraqi morale and prevented Saddam Hussein from bringing the strength of his army to bear against Coalition ground forces.⁷¹

Electrical Production Facilities. A modern military and industrial power such as Iraq, relies heavily on electricity. Attacks on Iraqi power facilities shut down their effective operations and eventually collapsed the national power grid. This produced a cascading effect making the destruction of some other facilities unnecessary. The strikes reduced or eliminated the reliable supply of electricity required to power nuclear, biological, and chemical weapons production facilities as well as other war-supporting industries. They eliminated the power needed to refrigerate bio-toxins and some chemical agents. They shut down the computer systems required to integrate the air defense network; to pump fuel and oil from storage facilities into trucks, tanks, and aircraft; to operate reinforced doors at aircraft storage and maintenance facilities; and to provide the lighting and power for maintenance, planning, repairs, and the loading of bombs and explosive agents. To do this effectively, the Coalition disrupted virtually the entire Iraqi electric grid otherwise the Iraqis could have rerouted power around the damaged nodes. Backup generators were certainly available but they are usually slow to come on line, provide less power than main sources, and are not as reliable. During the switch from main power to a backup generator, computers drop off line, temporary confusion ensues, and other residual problems occur. In the fast pace of a modern, massed air attack, even milliseconds of enemy power disruption can mean the difference between life and death for aircrews. The synergistic effect of losing primary electrical power sources in the first days of the war reduced Iraq's ability to respond to Coalition attacks and undoubtedly helped keep Coalition casualties low.⁷²

Telecommunications and Command, Control, and Communication Nodes. To effectively deploy and use his forces, Saddam Hussein required the critical ability to issue orders to military and security forces, to receive reports on the status of operations, and to communicate with senior political and military leaders. To challenge this ability, the Coalition bombed microwave relay towers, telephone exchanges, switching rooms, fiber optic nodes, and bridges carrying coaxial communications cables. Saddam Hussein's ability to transmit detailed, timely orders to his senior field commanders deteriorated rapidly. The physical destruction of his C3 capability began shortly before the initiation of the air war with attacks on key nodes of the air defense and C3 systems. It included destruction of the civil telecommunications system--an integral part of military communications supporting approximately sixty percent of military landline communications. Degrading this system immediately reduced Saddam's ability to command both military forces and secret police. Internal radio and television systems also provided lucrative targets. Saddam retained only marginal ability to broadcast outside the country and could broadcast only sporadically to his own people. This essentially limited the scope and effects of his PSYOP campaign.⁷³

Since Iraq could eventually repair its national-level communications capability, Coalition forces programmed continuous strikes. Although the network contained some built in redundancy, the backup systems offered a more vulnerable target for eavesdropping and, thus, presented a lucrative source of intelligence.⁷⁴

According to CENTCOM and EPW reports, communications between corps and division headquarters and their subordinate units along the Kuwait-Saudi border virtually ceased. Iraqi commanders resorted to messengers to communicate with other units and different command levels. Some captured Iraqi commanders indicated they had no contact at all with their higher headquarters for more than a week before the initiation of the ground offensive.⁷⁵

Strategic Integrated Air Defense System. On the eve of the air campaign, Iraq possessed a formidable IADS. It was dense, overlapping, and dangerous, a mix of Soviet and Western equipment including radars, interceptor aircraft, SAMs and AAA, tied together by Kari, the French-built,

computerized C2 system. The AAA used either radar or optical guidance; the SAMs employed either radar or infrared guidance. The AAA posed the greatest threat below 12,000 to 15,000 feet, while the SAMs provided overlapping coverage from virtually ground level to above 40,000 feet. Before Coalition forces could make maximum use of air power, they had to reduce the effectiveness of this extensive network. Accordingly, prime Iraqi targets included the middle- and upper-level air defense control centers, SAM sites, radar sites, and the C3 nodes that connected the system.⁷⁶

The first wave of Coalition attackers consisted of three separate groups that included F-117s and Tomahawk land-attack missiles (TLAM). Within the first five minutes, they struck nearly twenty air defenses, C3, electrical, and leadership nodes in Baghdad. Within an hour, they struck an additional twenty-five targets of a similar nature as well as electric distribution and chemical weapons facilities. By the close of the first twenty-four hours of the war, Coalition forces had damaged or destroyed almost four dozen key targets around the enemy capital. Their targets included more than a dozen leadership targets, a similar number of air defense and electric distribution facilities, and ten C3 nodes. The Coalition did not gradually shut down the Iraqi air defense system. They almost simultaneously struck so many vital centers that they virtually achieved instantaneous destruction of the network. Constant monitoring and restrikes ensured that the system never recovered.⁷⁷

Most hardened sector operations centers and intercept operations centers throughout the country ceased to function within the first few days of the air campaign. Their destruction left a crippled, fragmented system incapable of coordinated, integrated operations. Coalition strikes had so badly damaged the early warning radar net that Iraq was forced to rely on individual SAM battery radars to provide warning of attacks. Coalition aircraft operated at medium and high altitudes with virtual impunity. Not until the final few days of the war did aircraft losses increase. Air operations moved down into lower altitudes and encountered a higher threat posed by Iraqi battlefield defenses such as hand held infrared SAMs and small-caliber AAA.⁷⁸

Summary

In summary, the nature of Iraq's C2 system, compounded by specific weaknesses in its military force structure, offered some ideal targets that Coalition C2W planners adeptly exploited. The results were remarkable. On 3 March 1991, General Schwarzkopf met with senior Iraqi military officers to finalize the terms of the cease-fire. Present also was the Iraqi III Corps commander, leader of the Iraqi divisions occupying the eastern sector of the Kuwait-Saudi border and the Kuwaiti coastline. After discussing the status of Coalition prisoners of war (POW) in Iraqi hands, the Iraqis asked for an accounting of the Iraqi EPWs held by the Coalition. When informed that the number exceeded 58,000 and the count was incomplete, the Iraqi vice chief of staff, according to eyewitness accounts, appeared stunned. When he asked the III Corps commander if this were possible, the commander replied that it was possible, but he did not know. During discussion of a no-contact line to separate Coalition and Iraqi forces, the CINCCENT presented his proposed line. When the Iraqi vice chief of staff asked why it was drawn behind the Iraqi troops, Schwarzkopf explained that it was the forward line of the Coalition advance. The Iraqi officer again looked stunned. He again turned to the III Corps commander, who again replied that it was possible, but he did not know. Thus, three days after hostilities ended, the Iraqi senior military leadership still did not know where the Coalition forces were nor of the mass desertions of their forces. Their ignorance may in part reflect the weaknesses of a totalitarian system in which bad news travels slowly. However, it undoubtedly also testifies to the crippling of Iraqi command, control, communications, and intelligence by the synergistic application of deception, OPSEC, PSYOP, EW, and destruction in support of an aggressive air campaign and a bold and audacious ground operation.⁷⁹

Endnotes

¹Peter G. Tsouras, Warriors' Words: A Quotation Book (New York, NY: Arms and Armour Press, 1992), 407.

²Department of Defense, Conduct of the Persian Gulf War: Final Report To Congress (Washington, DC: U.S. Government Printing Office, 1992), 3.

³*Ibid.*, 3-4.

⁴*Ibid.*, 20.

⁵*Ibid.*, 71-72.

⁶*Ibid.*, 72.

⁷*Ibid.*

⁸FM 100-5 defines a center of gravity as "the hub of all power and movement upon which everything depends. It is that characteristic, capability, or location from which enemy and friendly forces derive their freedom of action, physical strength, or will to fight...The essence of operational art lies in being able to mass effects against the enemy's main source of power--his center of gravity, which he seeks to protect." Headquarters, Department of the Army, FM 100-5, Operations (Washington, DC: U.S. Government Printing Office, 1993), 6-7. Coalition planners identified three principle centers of gravity for the Iraq regime. In addition to Saddam Hussein's command, control, and leadership, they included Iraq's weapons of mass destruction, and the Republican Guard force.

⁹Conduct of the Persian Gulf War: Final Report To Congress, 72.

¹⁰*Ibid.*, 73.

¹¹*Ibid.*, 74.

¹²*Ibid.*, 75.

¹³*Ibid.*, 75-6.

¹⁴*Ibid.*, 187-8.

¹⁵*Ibid.*, 76-7.

¹⁶*Ibid.*, 105.

¹⁷AWACS: air surveillance and control provided by airborne early warning vehicles equipped with search and height-finding radar and communications equipment for controlling weapons.

¹⁸Conduct of the Persian Gulf War: Final Report To Congress, 105.

¹⁹*Ibid.*, 105-7.

²⁰Ibid., 212-19.

²¹Ibid., 222-3.

²²Ibid., 248.

²³Ibid.

²⁴Ibid.

²⁵Department of Defense, Conduct of the Persian Gulf Conflict: An Interim Report To Congress (Washington, DC: U.S. Government Printing Office, 1991), 24-2.

²⁶Ibid., 24-1.

²⁷Ibid.

²⁸Ibid.

²⁹Ibid.

³⁰Ibid., 24-2.

³¹Conduct of the Persian Gulf War: Final Report To Congress, 76-7.

³²An area of interest is "that area of concern to the commander, including the area of influence, areas adjacent thereto, and extending into enemy territory to the objectives of current or planned operations. This area also includes areas occupied by enemy forces who could jeopardize the accomplishment of the mission." (An area of influence is "a geographical area wherein a commander is directly capable of influencing operations by maneuver or fire support systems normally under his command or control.") Headquarters, Department of the Army, Field Manual No 101-5-1, Operational Terms and Symbols (Washington, DC: U.S. Government Printing Office, 1985), 1-5.

³³Conduct of the Persian Gulf War: Final Report To Congress, 240, 248.

³⁴Ibid., 249, 246.

³⁵James F. Dunnigan and Austin Bay, From Shield To Storm: High-Tech Weapons, Military Strategy, and Coalition Warfare in the Persian Gulf (New York: William Morrow and Company, Inc., 1992), 287.

³⁶Conduct of the Persian Gulf War: Final Report To Congress, 536-7.

³⁷Conduct of the Persian Gulf Conflict: An Interim Report To Congress, 5-3.

³⁸From Shield To Storm: High-Tech Weapons, Military Strategy, and Coalition Warfare in the Persian Gulf, 288.

³⁹Conduct of the Persian Gulf War: Final Report To Congress, 145.

⁴⁰4th Psychological Operations Group (Airborne), Leaflets of the Persian Gulf War (Fort Bragg, NC: 4th POG, undated), 8.

⁴¹Conduct of the Persian Gulf War: Final Report To Congress, 537-8.

⁴²Conduct of the Persian Gulf Conflict: An Interim Report To Congress, 5-3.

⁴³Leaflets of the Persian Gulf War, 1.

⁴⁴Conduct of the Persian Gulf War: Final Report To Congress, 538.

⁴⁵Conduct of the Persian Gulf Conflict: An Interim Report To Congress, 5-3.

⁴⁶Bruce W. Watson, Bruce George, Peter Tsouras, B.L.Cyr, and the International Analysis Group on the Gulf War, Military Lessons of the Gulf War (Russell Gardens, London: Lionel Leventhal Limited, 1993), 157.

⁴⁷*Ibid.*, 157-8.

⁴⁸*Ibid.*, 158.

⁴⁹Conduct of the Persian Gulf War: Final Report To Congress, 533.

⁵⁰Military Lessons of the Gulf War, 158-9.

⁵¹*Ibid.*

⁵²*Ibid.*

⁵³*Ibid.*, 159-60.

⁵⁴*Ibid.*

⁵⁵*Ibid.*

⁵⁶*Ibid.*

⁵⁷*Ibid.*, 161. See also Conduct of the Persian Gulf War: Final Report To Congress, 129.

⁵⁸*Ibid.*

⁵⁹*Ibid.*

⁶⁰*Ibid.*, 162.

⁶¹*Ibid.* See also Conduct of the Persian Gulf War: Final Report To Congress, 129.

⁶²*Ibid.*

⁶³Ibid., 162-3.

⁶⁴Ibid., 163.

⁶⁵Ibid.

⁶⁶Ibid.

⁶⁷Conduct of the Persian Gulf War: Final Report To Congress, 148.

⁶⁸The air campaign identified five military objectives: isolate and incapacitate the Iraqi regime; gain and maintain air supremacy to permit unhindered air operations; destroy nuclear, biological, and chemical warfare capabilities; eliminate Iraq's offensive military capability by destroying major parts of key military production, infrastructure, and power projection capabilities; render the Iraqi army and its mechanized equipment in Kuwait ineffective, causing its collapse.

⁶⁹Ibid., 95.

⁷⁰Ibid., 96, 150.

⁷¹Ibid., 229, 253.

⁷²Ibid., 96, 150.

⁷³Ibid., 96, 151.

⁷⁴Ibid., 151-2.

⁷⁵Ibid., 137-8.

⁷⁶Ibid., 96, 154.

⁷⁷Ibid., 117-118.

⁷⁸Ibid., 154.

⁷⁹Ibid., 160-1.

CHAPTER 4

CONCLUSIONS

The way of the warrior is to master the virtue of his weapons.¹

Myamoto mushaski, A Book of Five Rings

As chapter 3 has demonstrated, command and control warfare contributed significantly to the Coalition victory during the Gulf War. It enabled friendly forces to work inside the enemy commanders' decision cycles forcing them into a reactive set of actions, providing friendly commanders and forces strategic and tactical advantage on the battlefield. The war brought together the traditional components of C3CM--OPSEC, military deception, EW, and physical destruction--with an intensity and tempo heretofore unimagined. The most distinguishing aspect of this effort was the shift in focus from the counter-equipment concept of C3CM to C2W's strategy of attacking an entire information system, including the human element. The addition of PSYOP made targets of the "senders" and "receivers" within the Iraqi command structure and raised the strategy of C3CM to that of C2W--all-out war on the enemy's complete C2 system. It created something significantly more powerful than the sum of its individual pieces.²

In analyzing the application of C2W during the Gulf War, a number of issues surface that provide clues to its success and that carry import for the use of C2W in future operations. The purpose of this chapter is to examine those issues and to offer recommendations to optimize unit C2W programs.

Joint and Multinational

Like Desert Storm, tomorrow's battles will take place in a joint environment and one that will most likely be multinational. C2W is designed for such an environment; it leverages the needed

capabilities from the service or component who has them available and employs them to support the task force or combatant commander's mission. Just as there is a synergy in employing the five elements of C2W in a synchronized manner, there is a synergy in blending the capabilities of each service to focus on mission accomplishment.³ To achieve this synergism, C2W doctrine, planning, and training must have as a foundation commonly accepted concepts and terminology. A joint focus must replace the present service-specific array of concepts and terms to enable forces to exploit the inherent advantages of C2W (table 7) and avoid misunderstandings and communications breakdowns (table 8).

Centralized Control

C2W is most effective when the combatant commander or the joint task force commander centrally controls its planning and tasking. C2W obtains its greatest results when the commander focuses it on one purpose--achieving his strategic objectives-- rather than allowing it to be needlessly dispersed. C2W forces can easily lose their versatility when subordinate to other elements of power. Scarce assets are easily diverted to missions of marginal importance to the C2W strategy and C2W objectives can be ignored altogether.

During Desert Storm, the greatest impact of centralized control manifested in the deception operation. Prior to the launch of the ground offensive, commanders of forces oriented to the western sector of the area of operations would have preferred to position their forces as early as possible in the west and to conduct extensive reconnaissance and intelligence operations within their specific sectors. They would have sought air strikes to attrit enemy forces in their line of advance. Logistics elements would have stockpiled supplies farther west in preparation for the offensive. Although normal, prudent measures prior to an attack, these actions would have clearly revealed Coalition plans and compromised the deception story. Because he retained centralized control of the deception plan, General Schwarzkopf was able to ensure a unity of effort and prevent conflicting objectives, however valid, from compromising his strategic plan.

Table 7. Mutual Support Within C2W

SUPPORTED BY:	OPSEC	DECEPTION	PSYOP	DESTRUCTION	EW
OPSEC		<ul style="list-style-type: none"> o Conceal competing observables o Degrade general situation information to enhance effect of observables 	<ul style="list-style-type: none"> o Conceal competing information o Degrade general situation information to enhance effect of PSYOP 	<ul style="list-style-type: none"> o Conceal dedicated systems for counter-C2 to deny information on extent of its destruction capabilities 	<ul style="list-style-type: none"> o Conceal EW units and systems to deny information on extent of EA/ES capabilities
DECEPTION	<ul style="list-style-type: none"> o Influence adversary not to collect against protected units/activities o Influence adversary to underestimate friendly OPSEC o Provide information to fill gaps created by friendly OPSEC 		<ul style="list-style-type: none"> o Provide information compatible with PSYOP theme o Reinforce PSYOP theme in content of deception information 	<ul style="list-style-type: none"> o Influence adversary to: <ul style="list-style-type: none"> - underestimate friendly destruction capabilities - defend wrong C2 elements/systems from friendly detection and destruction 	<ul style="list-style-type: none"> o Influence adversary to: <ul style="list-style-type: none"> - underestimate friendly EA/ES capabilities - defend wrong C2 systems from friendly EA/ES
PSYOP	<ul style="list-style-type: none"> o Information projection in operations other than war o Create perceptions which fit OPSEC activities 	<ul style="list-style-type: none"> o Create perceptions and attitudes that can be exploited by military deception o Integrate PSYOP actions with deception 		<ul style="list-style-type: none"> o Cause populace to flee targeted areas, reducing collateral damage limitations on destruction of adversary C2 infrastructure 	<ul style="list-style-type: none"> o PSYOP broadcast assets disseminate products on adversary frequencies o Develop messages for broadcast on other service EW assets (e.g., AC-130)
DESTRUCTION	<ul style="list-style-type: none"> o Prevent or degrade adversary reconnaissance and surveillance against protected units and activities 	<ul style="list-style-type: none"> o Conduct physical attacks as deceptive executions o Degrade adversary capabilities to see, report, and process competing observables o Isolate decision maker from information at critical times to enhance effect of deception execution 	<ul style="list-style-type: none"> o Degrade adversary capability to see, report, and process conflicting information o Degrade adversary capability to jam PSYOP broadcast o Isolate target audience from conflicting information 		<ul style="list-style-type: none"> o Reduce friendly EA target set by selective and coordinated destruction of adversary C2 infrastructure targets o Destroy selected electronic systems to force adversary use of systems susceptible to friendly EA/ES
EW	<ul style="list-style-type: none"> o Degrade adversary reconnaissance and surveillance in EMS against protected units and activities o Cover short term gaps in OPSEC 	<ul style="list-style-type: none"> o Conduct EA/ES as deceptive executions o Degrade adversary capability to see, report, and process competing observables o Isolate decision maker from information at critical times to enhance effect of deception executions 	<ul style="list-style-type: none"> o Degrade adversary capability to see, report, and process conflicting information o Isolate target audience from conflicting information 	<ul style="list-style-type: none"> o Provide target acquisition through ES o Destroy or upset susceptible assets using EMS with EA 	

Source: Headquarters, Department of the Army, FM 100-6, Information Operations (Washington, DC: U.S. Government Printing Office, working draft, 1995), 3-25, figure 3-7.

Table 8. Conflicts Within C2W

CONFLICTS	OPSEC	DECEPTION	PSYOP	DESTRUCTION	EW
OPSEC		o OPSEC requirements may limit information that can be revealed to enhance credibility of deception story	o OPSEC requirements may limit information that can be revealed to develop PSYOP themes		
DECEPTION	o Deception story and associated executions may need to reveal information the OPSEC normally seeks to deny		o Deception story may limit selection of PSYOP themes o Deception story may limit information that can be revealed to develop PSYOP themes	o Deception executions may limit destructive targeting of the adversary C2 infrastructure to allow survival and conduct of critical adversary C2 functions	o Deception executions requiring EMS may limit EA targeting of the adversary C2 infrastructure to allow survival and conduct of critical adversary C2 functions
PSYOP	o PSYOP may need to reveal information that OPSEC normally seeks to deny (especially in operations other than war)	o PSYOP themes may limit selection of deception story o PSYOP may be limited by untruths in deception story		o PSYOP activities may limit destructive targeting of the adversary C2 infrastructure to allow PSYOP themes to be conveyed	o PSYOP activities requiring EMS may limit EA against selected adversary communications frequencies to allow PSYOP themes to be conveyed
DESTRUCTION		o Physical destruction may limit the selection of deception execution by denying or degrading elements of the adversary C2 infrastructure necessary to the deception	o Physical destruction may limit the selection of means to convey PSYOP themes by denying or degrading elements of the adversary C2 infrastructure necessary to convey PSYOP messages		o Physical destruction may limit opportunities for communications intrusion by denying or degrading elements of the adversary C2 infrastructure necessary to communication intrusion
EW		o EA may limit the selection of deception executions by denying or degrading the use of certain electronic systems in the adversary C2 system	o EA may limit the selection of means to convey PSYOP themes by denying or degrading the use of certain adversary or target audience communication frequencies	o EA activities may limit destructive targeting of the adversary C2 infrastructure to allow PSYOP themes to be conveyed	

Source: Headquarters, Department of the Army, FM 100-6, Information Operations (Washington, DC: U.S. Government Printing Office, working draft, 1995), 3-26, figure 3-8.

Decentralized Execution

Conversely, the commander should decentralize the execution of C2W missions to achieve effective spans of control and to ensure responsiveness and tactical flexibility. At each level, commanders employed available C2W to disrupt the Iraqi's perceived centers of gravity. Targets included: enemy command elements at all echelons; war production assets, particularly nuclear,

biological and chemical (NBC) facilities; supporting infrastructure such as bridges housing communications lines and servicing resupply routes, air defense radar networks, and electrical production facilities; the communications infrastructure from strategic to tactical levels; and the perceptions of the individual Iraqi soldier. Coalition forces effectively operated inside the Iraqi leaders' decision cycles, forcing them to take reactive measures while friendly forces exploited strategic and tactical advantages on the battlefield.

Integration of Effort

C2W is a complex undertaking. It encompasses activities which cut across all the major functions performed by forces on the battlefield and contains five diverse elements. Proper synchronization is essential to successful C2W execution.⁴ The real-time coordination of the various C2W actions performed by the Coalition forces was a key factor in the success of C2W during the Gulf War. This integration represented a significant change from the use of C2W capabilities in previous conflicts. For although U.S. military forces have long possessed and employed the elements of C2W, they have used them individually, and have had neither the doctrine nor the inspiration to envision a coordinated, integrated strategy. The Gulf War demonstrated the relevance and effectiveness of such an approach.

The integrated air campaign and the marine amphibious activities along the coast are an example. They kept Iraqi forces fixated toward the Kuwaiti coast and prevented Iraqi airborne reconnaissance assets from leaving the ground while OPSEC and deception measures employed by forces along the Kuwait-Saudi border presented a false picture of Coalition intentions. In concert, these actions enabled the undetected shift of forces to the west. Iraqi commanders did not know the direction or the timing of the Coalition attack until well after its launch.

Intelligence Support

Accurate and timely intelligence is essential to the success of C2W. No other nation or alliance of nations has had the ability that Coalition forces possessed during the Gulf War to collect

information and disseminate intelligence. No combat commander has had as full and complete a view of his adversary as did the Coalition field commanders.⁵ However, the aftermath of the Cold War gives rise to obstacles which may hinder that level of support in future operations. The proliferation of potential adversaries magnifies the problem of collecting and processing the information needed to protect against enemy C2W capabilities. At the same time, commercial off-the-shelf information technologies have become so readily available, they expand and complicate the task of information support to friendly C2W efforts. Additionally, the efforts of the intelligence community appear centered on high-technology sources. Elements of the C2W strategy, notably PSYOP and deception, depend heavily on intelligence gained from human sources. Human intelligence (HUMINT) reveals enemy deception plans and offers feedback on the effectiveness of friendly deception strategies. It provides psychological profiles on enemy leaders and offers clues to the morale and will to fight of enemy forces. It produces potential PSYOP themes as well as indicating those of an enemy. Advanced sensor technology and space-based systems provide essential data on enemy force locations and the operating parameters of their equipment but they cannot reveal how those decision makers process and use the information available to them. Knowledge of an opponent's C2 infrastructure provides lucrative targets but cannot offer predictions on how those targets--the enemy commanders and staffs--are influenced or affected by friendly C2W actions. Advanced technological capabilities provide invaluable information but they cannot replicate HUMINT's contribution to C2W. Unfortunately, HUMINT suffers from a relatively low priority in the U.S. collection strategy.⁶

Training

The military has long emphasized the need to "train as we are going to fight." C2W is no exception. Unfortunately, exercises frequently exclude EW operations due to their potential for confusion and interference. Safety concerns preclude the use of directed energy weapons. The scope of the exercise as well as lack of skilled personnel restrict meaningful PSYOP and deception play. OPSEC frequently functions in a lock-step fashion without real command involvement.⁷ If soldiers are to contribute to the C2W effort, training programs must focus on building a foundation in their

individual disciplines. Operators and soldiers must learn new skills in adjusting to alternative battlefield environments to make them fully capable of performing the tasks that arise as new C2W methods and systems are perfected. However, this training is only the beginning. To be effective, C2W training must center on the commanders and staff officers who direct, plan, and control the variety of activities required to attain C2W objectives.⁸

Current and projected training systems in all spheres of military activity must include the new C2W environment. Exercises, simulations, and training sessions must provide a realistic training environment in which to practice and hone these skills, particularly those of commanders and their staffs. This offers a particularly difficult challenge to both simulation designers and trainers who must replicate an integrated C2W planning and execution capability for all levels of friendly and opposing forces in a wide variety of training environments.⁹

Recommendations

The successful employment of C2W rests with a number of factors discussed throughout this thesis. Historical accounts of battles ranging from a distant past to the most recent contingencies offer C2W lessons to commanders and their staffs as well as individual soldiers. The following summarizes the key recommendations:

1. Ensure the focus on C2W encompasses a joint perspective, employing commonly understood concepts and terminologies that span the services.
2. Maintain central control of C2W planning and tasking at the joint task force or combatant command level; decentralize the execution. Focus the overall C2W strategy on meeting that commander's strategic objectives; avoid needless dispersion of scarce assets.
3. At the same time, ensure that C2W is part of the strategy and campaign thinking at all levels of war--strategic, operational, and tactical.
4. Ensure adequate intelligence support. In particular, battle damage assessments must include methods to assess the effectiveness of deception and PSYOP operations and how they impact the minds of enemy commanders.

5. Include C2W in professional military education programs. At the basic training level introduce inductees and student officers to the concept of C2W, its associated elements, and its value on the battlefield. Provide more detailed training during first-level professional military education courses, stressing C2W's support to combat operations at the strategic, operational, and tactical levels of war. At mid-level professional military education courses introduce instruction on planning and executing a C2W strategy. At senior-level courses and senior leadership warfighting courses stress the role of command emphasis in integrating and synchronizing a C2W strategy to support command objectives.

Summary

The history of warfare is a never-ending story of change. Technological advancements have continuously refined and improved weaponry and weapons systems, doctrine and tactics have hastened to adapt to each new development, and the cycle endlessly repeats. Technological changes have altered the character of war more profoundly in the last two centuries than ever before. The railroad, telegraph, steam-powered ironclad, and rifle engendered dramatic increases in military effectiveness between the Napoleonic wars and the American Civil War. Prior to World War I, similar changes accompanied the introduction of the machine gun, the airplane, and the submarine. By the advent of World War II, the internal combustion engine, improved aircraft, radio, and radar initiated revolutionary leaps in long-range, highly mobile operations such as blitzkrieg and carrier air strikes. At the end of World War II, the development of nuclear weapons and their subsequent mating with ballistic missiles marked perhaps the most profound revolution in military affairs (RMA) to date.

In the early 1980s, the Soviets hypothesized the emergence of a new RMA, one that relied on advanced non-nuclear technologies and incorporated information sciences into the military sphere. The events of the Gulf War convinced them of the validity of their beliefs and, in fact, confirmed that a new RMA is emerging--one based heavily on information processing and stealthy long-range precision strike weapons.¹⁰ The "miracles" of this new wave of technology are considerable, providing

an unparalleled availability of real-time information that enables commanders to better dominate their battle space.

Although information processing has always been part of warfare, as the world enters the information age it becomes central to the outcome of battles and engagements. Friendly knowledge of the enemy and situational awareness must be more certain, more timely, and more accurate than the adversary's. As the Gulf War amply demonstrated, C2W enables the commander to achieve information dominance and to exploit its battlefield advantages, forcing the enemy to become reactive and to cede the initiative.

C2W involves more than technological superiority. Technology is critical in providing a capability to gain battlefield advantages; however it is the art of war that enables the commander to exploit these capabilities, to provide victory in the least amount of time with minimal loss of life and expenditure of resources. Just as command and control is more than simply communications, computers, and data, C2W is not merely jammers, zappers, decoys, and an arsenal of brilliant munitions. Equating C2W solely to technology is equivalent to defining the essence of maneuver as tanks, helicopters, infantry fighting vehicles, and trucks. Maneuver relies on those elements, but it is the commander's skill in employing them that provides the decisive advantage.¹¹ The same holds true for C2W; its success depends upon the skill of the commanders, staffs, and individuals who plan and direct the C2W strategy and who operate its systems and equipment.

C2W focuses on command and control--the functions military commanders and their staffs rely on to organize and conduct operations. C2W targets those decision makers and the information processes that support them. It seeks out sensors, communications, computers, and command posts to reach these primary targets.¹² The coordinated use of the elements of C2W creates a synergistic effect which gives commanders the capability to deliver a decisive blow to an opponent's command and control system. Without effective C2, enemy forces lose any ability to fight as a coordinated whole. Unable to achieve the desired initiative, the enemy commanders must resort to a reactive mode of operation. It is the skillful, integrated employment of its five elements that gives C2W its

power on the battlefield. Commanders, staffs, and individuals must know the role they each play. The key to this awareness is training.

Historical accounts abound with examples of the advantages obtained when commanders have skillfully employed OPSEC, deception, EW, PSYOP, and destruction. An equal number of records testify to the disastrous results possible when the leadership ignores those tools. Desert Storm dramatically demonstrated that the greatest effects arise from the integration of those elements into a mutually supportive, synergistic strategy that combines the talents of each military service to achieve one overall objective--the disruption of enemy C2 and the protection of friendly C2. C2W made a decisive difference in the Gulf War; properly understood and employed, it will help achieve victories on future battlefields. The key to its effectiveness is training. Commanders, staffs, and individuals must understand its concepts and the role they play in making it work. That understanding comes through training and practice.

As the military teeters on the edge of the Information Age, the "miracles" of technology are considerable. However, the value of the human mind does not diminish. No matter how sophisticated the technology or how many tasks are turned over to computers, technology will never completely replace the human element. Success or failure on the battlefield may be enhanced by technology, but it will be guaranteed by human ingenuity.

Endnotes

¹Justin Wintle, ed., The Dictionary of War Quotations (New York, NY: The Free Press, 1989), 45.

²Jim Gray, "Turning Lessons Learned into Policy," Journal of Electronic Defense (October 1993), 88-90.

³Headquarters, Department of the Army, FM 100-6, Information Operations (Washington, DC: U.S. Government Printing Office, working draft, 1995), 3-27-3-28.

⁴*Ibid.*, 3-27.

⁵Department of Defense, Conduct of the Persian Gulf Conflict: An Interim Report To Congress (Washington, DC: U.S. Government Printing Office, 1991), 14-1.

⁶Kerry A. Blout and Lauren D. Kohn, "C2 Warfare in FM 100-6," Military Review LXXV, no. 4 (July-August 1995): 68.

⁷FM 100-6, Information Operations, 3-28.

⁸Blout and Kohn, 68.

⁹*Ibid.*

¹⁰James R. Fitzsimonds and Jan M. Van Tol, "Revolutions in Military Affairs," Joint Forces Quarterly (Washington, DC: National Defense University, Spring 1994, Number 4), 25-7.

¹¹Blout and Kohn, 67.

¹²*Ibid.*

BIBLIOGRAPHY

Books

- Burnod, Akerly J., ed. Military Maxims of Napoleon. New York: Wiley and Putnam, 1845.
- Donnelly, Thomas, Margaret Roth, and Caleb Baker. Operation Just Cause: The Storming of Panama. New York: Macmillan, Inc., 1991.
- Dunnigan, James F., and Austin Bay. From Shield To Storm: High-Tech Weapons, Military Strategy, and Coalition Warfare in the Persian Gulf. New York: William Morrow and Company, Inc., 1992.
- Hastings, Max. Overlord: D-Day and the Battle For Normandy. New York: Simon and Schuster, Inc., 1984.
- Schwartz, Winn. Information Warfare: Chaos on the Electronic Superhighway. New York: Thunder's Mouth Press, 1994.
- Toffler, Alvin, and Heidi Toffler. War and Anti-War: Survival at the Dawn of the 21st Century. New York: Little, Brown and Company, 1993.
- Tsouras, Peter G. Warriors' Words: A Quotation Book. New York: Arms and Armour Press, 1992.
- Watson, Bruce W., Bruce George, Peter Tsouras, and B.L. Cyr. Military Lessons of the Gulf War. California: Presidio Press, 1993.
- Wintle, Justin, ed. The Dictionary of War Quotations. New York: The Free Press, 1989.

Government Documents

- Chairman, Joint Chiefs of Staff. Joint Pub. 1-02, Department of Defense Dictionary of Military and Associated Terms. Washington, DC: U.S. Government Printing Office, December 1989.
- _____. Joint Pub 3-0, Doctrine For Joint Operations. Washington, DC: U.S. Government Printing Office, 1993.
- _____. Joint Pub 3-13, Joint Command and Control Warfare (C2W) Operations. Washington, DC: U.S. Government Printing Office, December 1989.
- _____. Joint Pub 3-13.1, Joint Doctrine For Command and Control Warfare (C2W). Washington, DC: U.S. Government Printing Office, February 1996.

- _____. Joint Pub 3-53, Doctrine For Joint Psychological Operations. Washington, DC: U.S. Government Printing Office, July 1993.
- _____. Joint Pub 3-54, Joint Doctrine For Operations Security. Washington, DC: U.S. Government Printing Office, August 1991 with Change 1 dated 1 April 1994.
- _____. Joint Pub 3-58, Joint Doctrine For Military Deception. Washington, DC: U.S. Government Printing Office, June 1994.
- _____. Memorandum of Policy No. 30, Command and Control Warfare. Washington, DC: U.S. Government Printing Office, March 1993.
- Department of Defense. Conduct of the Persian Gulf Conflict: An Interim Report to Congress. Washington, DC: U.S. Government Printing Office, July 1991.
- _____. Conduct of the Persian Gulf War: Final Report to Congress. Washington, DC: U.S. Government Printing Office, April 1992.
- Headquarters, 4th Psychological Operations Group (Airborne). Leaflets of the Persian Gulf War. Fort Bragg, NC: 4th PSYOP Group, undated.
- Headquarters, 8th Psychological Operations Battalion. Building Bridges: Commander's Guide to Face to Face Communication. Fort Bragg, NC, undated.
- National Defense University. Joint Command and Control Warfare Staff Officer Course: Student Text. Norfolk, VA: Armed Forces Staff College, April 1993.
- School of Information Warfare and Strategy. Definitions for the Discipline of Information Warfare and Strategy. Washington, DC: National Defense University, 1994-95.
- _____. "Information-Based Warfare: An Annotated Bibliography," Draft, Unedited. Washington, DC: National Defense University, August 1994.
- United Task Force Somalia, Joint Psychological Operations Task Force. Psychological Operations in Support of Operation Restore Hope. FPO AP 96608-3606: JPOTF, May 1993.
- US Army. FM 90-2, Battlefield Deception. Washington, DC: U.S. Government Printing Office, 1988.
- _____. FM 100-5, Operations. Washington, DC: U.S. Government Printing Office, June 1993.
- _____. FM 100-6, Information Operations Draft, Unedited. Washington, DC: U.S. Government Printing Office, July 1995.
- _____. TRADOC Pamphlet 525-5, Force XXI Operations. Fort Monroe, VA: Army Training and Doctrine Command, August 1994.
- _____. TRADOC Pamphlet 525-69, Military Operations: Concept For Information Operations. Fort Monroe, VA: Army Training and Doctrine Command, August 1995.

Periodicals

- Ackerman, Robert K. "Military Planners Gird for Information Revolution." Signal (May 1995): 71-77.
- Amarante, José Carlos Albano do. "The Automated battle: A Feasible Dream?" Military Review vol. LXXIV, no. 5 (May 1994): 58-61.
- "Army Plan Fosters Dynamic Information War Framework." Signal vol. 48, no. 3 (November 1993): 55-58.
- Blount, Kerry A., and Lauren D. Kohn. "C2 Warfare in FM 100-6." Military Review vol. LXXV, no. 4 (July-August 1995): 66-69.
- Boorda, Jeremy M. "Leading the Revolution in C4I." Joint Forces Quarterly (Autumn 1995): 14-17.
- Campen, Alan D. "Information Warfare is Rife With Promise, Peril." Signal vol. 48, no. 3 (November 1993): 19-21.
- _____. "Rush to Information-Based Warfare Gambles with National Security." Signal (July 1995): 67-69.
- _____. "Cooperative Effort Encourages Safe Information Highway Travel." Signal vol. 50, no. 2 (October 1995): 43-44.
- DeGroat, Arthur S., and David C. Nilsen. "Information and Combat Power on the Force XXI Battlefield." Military Review vol. LXXV, no. 6 (November-December 1995): 56-62.
- FitzGerald, Mary C. "Russian Views on Electronic Signals and Information Warfare." American Intelligence Journal (Spring/Summer 1994): 81-87.
- FitzSimonds, James R., and Jan M. van Tol. "Revolutions in Military Affairs." Joint Force Quarterly no. 4 (Spring 1995): 24-31.
- Garfinkel, Simson L. "The Manchurian Printer." The Boston Sunday Globe, 5 (March 1995): 83.
- Gray, Jim. "Turning Lessons Learned into Policy." Journal of Electronic Defense vol. 16, no. 10 (October 1993): 87-91.
- Grier, Peter. "Information Warfare." Air Force Magazine (March 1995): 34-37.
- Hingtgen, David L. "Honing Information Warfare Skills." Space Tracks (Spring 1995): 24.
- Horner, Charles A. "The Air Campaign." Military Review vol. LXXI, no. 9 (September 1991): 16-27.
- "Information Operations." Military Review vol. LXXV, no. 6 (November-December 1995): 2.
- "It's All About The Information." The OPSEC Indicator 4 (Fall 1994): 1-2.

- Jensen, Owen E. "Information Warfare: Principles of Third-Wave War." Airpower Journal vol. VIII, no. 4 (Winter 1994): 35-44.
- Johnson, Craig L. "Information Warfare--Not a Paper War." Journal of Electronic Defense (August 1994): 55-58.
- Koch, Maj. James R. "Operation Fortitude: The Backbone of Deception." Military Review vol. LXXII, no. 3 (March 1992): 66-77.
- Kraus, George F., Jr. "Information Warfare in 2015." Proceedings (August 1995): 42-45.
- Libicki, Martin C. "What Is Information Warfare?" Strategic Forum no. 28 (May 1995): 1-4.
- Libicki, Martin C. and James A. Hazlett. "Do We Need An Information Corps?" Joint Force Quarterly no. 2 (Autumn 1993): 88-97.
- Macedonia, Michael R. "Information Technology in Desert Storm." Military Review vol. LXXII, no. 10 (October 1992): 34-41.
- Mann, Edward. "Desert Storm: The First Information War?" Airpower Journal vol. VIII, no. 4 (Winter 1994): 4-14.
- Matthys, Erick T. "Harnessing Technology for the Future." Military Review vol. LXXV, no. 3 (May-June 1995): 71-76.
- McKillip, J. D. "Iraqi Strategy During the Gulf War: An Alternate Viewpoint." Military Review vol. LXXV, no. 5 (September-October 1995): 46-51.
- Morris, Chris, Janet Morris, and Thomas Baines. "Weapons of Mass Protection: Nonlethality, Information Warfare, and Airpower in the Age of Chaos." Airpower Journal vol. IX, no. 1 (Spring 1995): 15-29.
- O'Connell, Edward P. "Nonlethal Concepts: Implications for Air Force Intelligence." Airpower Journal vol. VIII, no. 4 (Winter 1994): 26-34.
- Ryan, Donald E. "Implications of Information-Based Warfare." Joint Force Quarterly no. 6 (Autumn/Winter 1994-95): 114-116.
- Riccardelli, Richard F. "The Information and Intelligence Revolution." Military Review vol. LXXV, no. 5 (September-October 1995): 82-87.
- Shulter, Philip D. "Thinking About Warfare." Marine Corps Gazette 12 (November 1987): 18-26.
- Stein, George J. "Information Warfare." Airpower Journal vol. IX, no. 1 (Spring 1995): 30-55..
- Struble, Dan. "What Is Command and Control Warfare?" Naval War College Review vol. XLVIII, no. 3 (Summer 1995): 89-98.
- Summers, Harry Jr. "Full Circle: World War II to the Persian Gulf." Military Review vol. LXXII, no. 2 (February 1992): 38-48.

"Tracking the Storm." Military Review vol. LXXI, no. 9 (September 1991): 65-108.

Wallace, John, and Jim Jones. "Information Warfare/Information Operations (IO/TW) Update." The Air Land Sea Bulletin no. 96-1 (April 1996): 15-16.

Wardynski, E. Casey. "The Labor Economics of Information Warfare." Military Review vol. LXXV, no. 3 (May-June 1995): 56-61.

Washington, Douglas Waller. "Onward Cyber Soldiers." Time Magazine (August 1995): page unknown.

Wood, John R. "Lessons Learned in Information Age Warfare." Army 46 (February 1996): 32-44.

Yeosock, John J. "Army Operations in the Gulf Theater." Military Review vol. LXXI, no. 9 (September 1991): 2-15.

Unpublished Dissertations, Theses, and Papers

Czerwinski, Thomas J. "Information-Based Warfare: The Command Component at the Crossroads." 1994 Symposium on Command and Control Research and Decision Aids, Naval Postgraduate School, Monterey, CA, 1994.

Garrity, Patrick J. "Why the Gulf War Still Matters: Foreign Perspectives on the War and the Future of International Security." Center for National Security Studies, Los Alamos National Laboratory, 1993.

Grymes, Robert D. "Command and Control Warfare in Forced Entry Operations." Monograph, School of Advanced Military Studies, US Army Command and General Staff College, 1995.

Hutcherson, Norman B. "Command & Control Warfare: Putting Another Tool in the War-Fighter's Data Base." Research Report No. AU-ARI-94-1, Airpower Research Institute, 1994.

Kahan, James P., D. Robert Worley, and Cathleen Stasz. "Understanding Commanders' Information Needs." Research Report R-3761-A prepared for US Army by Rand Corporation.

Kay, David. "Denial and Deception: The Iraqi Weapons of Mass Destruction Program." Monograph prepared for DDI Seminar Series, undated.

Libicki, Martin C. "What is Information Warfare?" (draft) Advanced Command Concepts and Technology Institute for National Strategic Studies, National Defense University, 1995.

Marsh, Howard S. "From the Fog of War to Information Overload: A New Challenge for Command and Control." 1994 Symposium on Command and Control Research and Decision Aids, Naval Postgraduate School, Monterey, CA, 1994.

Murray, Thomas H. "OPSEC, Deception, and Cognition." Report prepared for Central

Intelligence Agency by Sequoia Associates, Inc., 1993.

Science Applications International Corporation. "Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance." Research report for the Chief, Information Warfare Division, Command, Control, Communications and Computer Systems Directorate, Joint Staff, Pentagon, 1995.

Smith, Kevin B. "The Crisis and Opportunity of Information War." Monograph, School of Advanced Military Studies, US Army Command and General Staff College, 1994.

Stein, George J. "Information War-Cyberwar-Netwar." Air University, Air War College, undated.

Swider, Gregory M., Charles H. Voas, Lloyd W. Koenig, and Barbara J. Lingberg. "Assessing the Tactical Value of Information." 1994 Symposium on Command and Control Research and Decision Aids, Naval Postgraduate School, Monterey, CA, 1994.

On-Line Sources

Cohen, Frederick B. (1993) "Information Warfare Considerations." [On-line], Available: <http://all.net/books/iw/iwardoc.html>

Fogleman, Ronald R. (1995, May 16) "Fundamentals of Information Warfare--An Airman's View." [On-line], Available: <http://all.net/books/iw/fogel.html>

Haeni, Reto E. (1995, December) "An Introduction to Information Warfare." [On-line], Available: <http://www.seas.gwu.edu/student/reto/infowar/info-war.html>

Magsig, Daniel E. (1995, December 7) "Information Warfare in the Information Age." [On-line], Available: <http://www.seas.gwu.edu/student/dmagsig/infowar.html>

Szafranski, Richard. (1996, April 23) "A Theory of Information Warfare: Preparing For 2020." [On-line], Available: <http://www.cdsar.af.mil/apj/szfran.html>

INITIAL DISTRIBUTION LIST

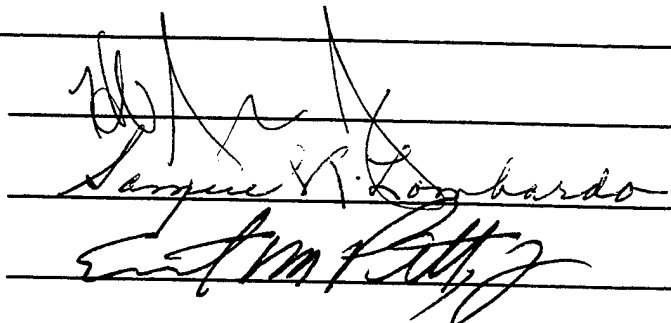
1. Combined Arms Research Library
U.S. Army Command and General Staff College
Fort Leavenworth, KS 66027-6900
2. Defense Technical Information Center
Cameron Station
Alexandria, VA 22314
3. LTC Herbert F. Merrick, Jr.
CDT
USACGSC
1 Reynolds Ave.
Fort Leavenworth, KS 66027-1352
4. LTC Samuel R. Lombardo
Dept BSL (MADN-L)
U.S. Military Academy
West Point, NY 10996-1784
5. COL Ernest M. Pitt, Jr.
3021 Lucille St.
Ashland, KY 41102
6. Joint Command and Control Warfare Center
Attn: DT
2 Hall Blvd Ste 217
San Antonio, TX 78243-7008
7. Training and Doctrine Command
Attn: DCSDOC
37 Fenwick Road
Fort Monroe, VA 23651
8. Joint Staff
Information Warfare & Special Technical Operations Division
3000 Joint Staff, The Pentagon
Washington, D.C. 20318-3000
9. Armed Forces Staff College
Joint C2W School
7800 Hampton Blvd
Norfolk, VA 23511-1702

10. U.S. Army Intelligence School
Training and Doctrine Directorate
Fort Huachuca, AZ 85613-5000
11. U.S. Army Information Systems Command
Attn: LIWA
8825 Beulah Street
Fort Belvoir, VA 22060-5246
12. Combined Arms Center
Attn: ATZL-TPIO-ABCS
415 Sherman Ave
Fort Leavenworth, KS 66027

CERTIFICATION FOR MMAS DISTRIBUTION STATEMENT

1. Certification Date: 07 / 05 / 96
2. Thesis Author: MAJOR ELIZABETH A. HURST
3. Thesis Title: SHAPING THE BATTLEFIELD WITH COMMAND AND CONTROL WARFARE

4. Thesis Committee Members Signatures:



5. Distribution Statement: See distribution statements A-X on reverse, then circle appropriate distribution statement letter code below:

☒ A B C D E F X SEE EXPLANATION OF CODES ON REVERSE

If your thesis does not fit into any of the above categories or is classified, you must coordinate with the classified section at CARL.

6. Justification: Justification is required for any distribution other than described in Distribution Statement A. All or part of a thesis may justify distribution limitation. See limitation justification statements 1-10 on reverse, then list, below, the statement(s) that applies (apply) to your thesis and corresponding chapters/sections and pages. Follow sample format shown below:

S	-----SAMPLE-----		SAMPLE-----		S	
A	<u>Limitation Justification Statement</u>	/	<u>Chapter/Section</u>	/	<u>Page(s)</u>	A
M						M
P	<u>Direct Military Support (10)</u>	/	<u>Chapter 3</u>	/	<u>12</u>	P
L	<u>Critical Technology (3)</u>	/	<u>Sect. 4</u>	/	<u>31</u>	L
E	<u>Administrative Operational Use (7)</u>	/	<u>Chapter 2</u>	/	<u>13-32</u>	E
	-----SAMPLE-----		SAMPLE-----			

Fill in limitation justification for your thesis below:

<u>Limitation Justification Statement</u>	<u>Chapter/Section</u>	<u>Page(s)</u>
	/	/
	/	/
	/	/
	/	/
	/	/

7. MMAS Thesis Author's Signature: Elizabeth A. Hurst

STATEMENT A: Approved for public release; distribution is unlimited. (Documents with this statement may be made available or sold to the general public and foreign nationals).

STATEMENT B: Distribution authorized to U.S. Government agencies only (insert reason and date ON REVERSE OF THIS FORM). Currently used reasons for imposing this statement include the following:

1. Foreign Government Information. Protection of foreign information.
2. Proprietary Information. Protection of proprietary information not owned by the U.S. Government.
3. Critical Technology. Protection and control of critical technology including technical data with potential military application.
4. Test and Evaluation. Protection of test and evaluation of commercial production or military hardware.
5. Contractor Performance Evaluation. Protection of information involving contractor performance evaluation.
6. Premature Dissemination. Protection of information involving systems or hardware from premature dissemination.
7. Administrative/Operational Use. Protection of information restricted to official use or for administrative or operational purposes.
8. Software Documentation. Protection of software documentation - release only in accordance with the provisions of DoD Instruction 7930.2.
9. Specific Authority. Protection of information required by a specific authority.
10. Direct Military Support. To protect export-controlled technical data of such military significance that release for purposes other than direct support of DoD-approved activities may jeopardize a U.S. military advantage.

STATEMENT C: Distribution authorized to U.S. Government agencies and their contractors: (REASON AND DATE). Currently most used reasons are 1, 3, 7, 8, and 9 above.

STATEMENT D: Distribution authorized to DoD and U.S. DoD contractors only; (REASON AND DATE). Currently most used reasons are 1, 3, 7, 8, and 9 above.

STATEMENT E: Distribution authorized to DoD only; (REASON AND DATE). Currently most used reasons are 1, 2, 3, 4, 5, 6, 7, 8, 9, and 10.

STATEMENT F: Further dissemination only as directed by (controlling DoD office and date), or higher DoD authority. Used when the DoD originator determines that information is subject to special dissemination limitation specified by paragraph 4-505, DoD 5200.1-R.

STATEMENT X: Distribution authorized to U.S. Government agencies and private individuals of enterprises eligible to obtain export-controlled technical data in accordance with DoD Directive 5230.25; (date). Controlling DoD office is (insert).